SECURITY AND FORENSIC TOOLS

FORENSIC CASE STUDY – Stockholm Case

INDIVIDUAL WRITTEN REPORT ON A FORENSIC CASE STUDY

WORD COUNT: 3250

ABSTRACT

The purpose of this paper is to go over the Stockholm Case investigation techniques and results. This case study examines data from a computer's hard drive or other storage devices, utilising established rules and processes to discover if they contain damning information. The forensic investigation was done utilising a virtual computer and a variety of digital forensic technologies. The purpose of this report is to outline the examination procedure and investigate data recovery from its source so that it can be broken down and reported in a logical manner.

CASE BACKGROUND

Nathan Spire's user information was created on a disc /D on May 11th, 2020. The offender, Nathan Spire, and his partner were accused of executing a scam operation in which he pretended to give Microsoft help to his victims. Nathan Spire and his partner exchanged multiple emails before to the fraud, outlining how to target the victims and get access into their system and collect money in gift cards. Nathan was caught defrauding one of his victims, 'Sara Hoyle,' by claiming to be able to fix her computer and then demanding payment in gift cards.
This case was investigated using:

1. Encase
2. Autopsy
3. Veracrypt
4. Openstego
5. Sonic Visualizer

These tools were used to retrieve information such as document files, images, Emails, and encrypted files from the hard drive that contained the evidence, including conversations between the two suspects.

1. Nathan Spire
2. Bossoftheoperation

This case holds information from bossoftheoperation to Nathan, and it is evident they have the motive to scam people using various methods and collect payments in giftcard methods.

Evidence Victims Nathan scammed found in Case:

1. Sara Hoyle

EXAMINATION OF THE CASE

On May 9th, 2022, at 14:47:07 BST. The Stockholm Case disc's forensic acquisition phase. Before photographing the disc, the date and characteristics were registered and gathered. The chain of custody was maintained as many pieces as possible of evidence were obtained. The case's Message Direct 5 verification was noticed, as well as various hash algorithms employing enclose. The MD5 was acquired and validated as a match, indicating that the file integrity has been confirmed. Because a dual verification is required before moving on to the next level of the study, autopsy was also employed to validate the picture.

MD5 od the D disk – 0a99db44332729de1971a35e3a25fdc5
SHA1 - 18c6616de55c77565810e4b9d14c2254d3f1c732

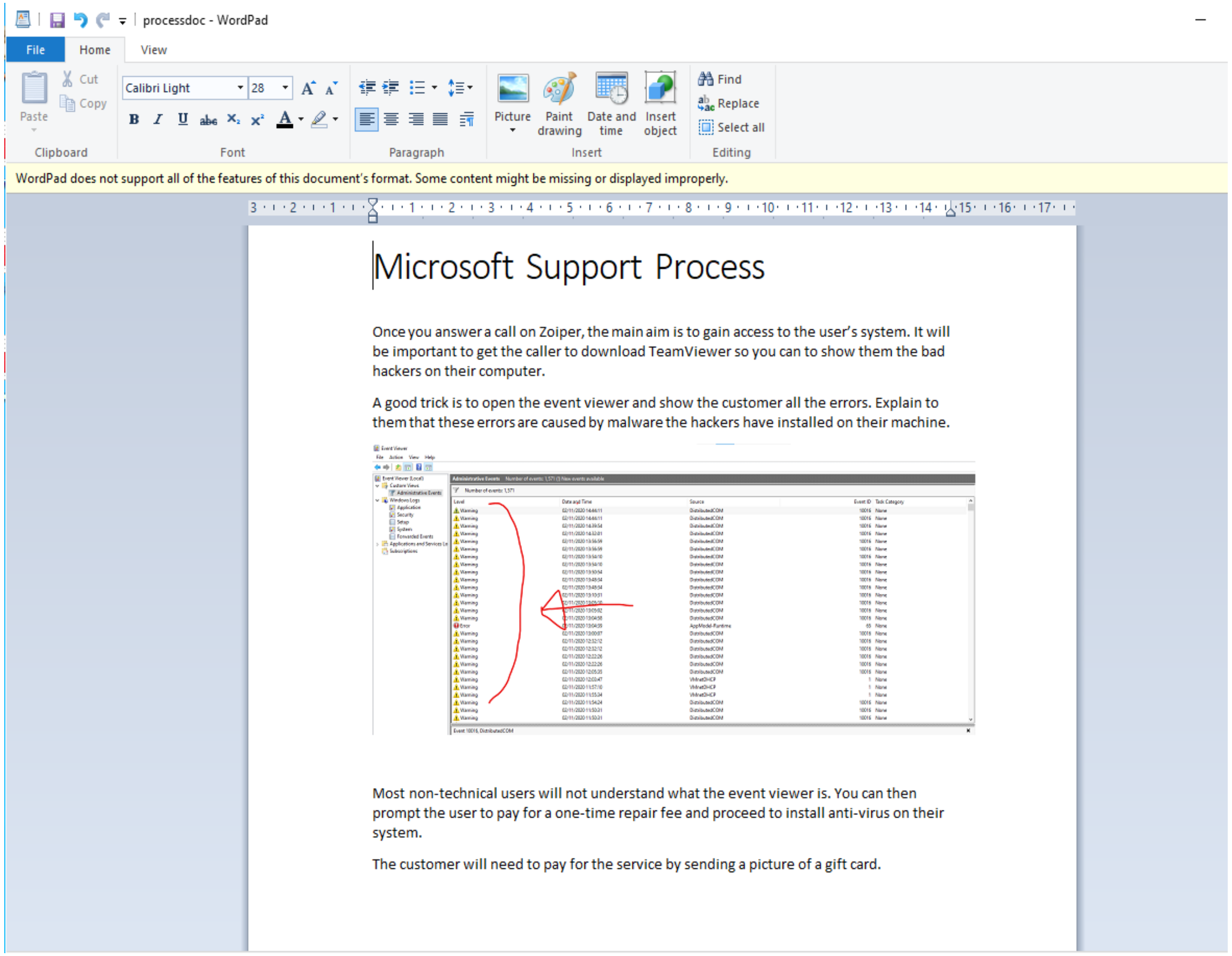
During the investigative stage of the case, various information and evidence were discovered, and the appropriate steps were followed to complete the forensic case study, including hash analysis, encrypted documents, audio recordings, and stegged photographs. On the Stockholm case, some emails were also discovered.
The Encase evidence processor and Autopsy were used to extract the evidence. Unallocated space, lost data, Internet artefacts, and emails are all examples of unallocated space. To get important information, this investigation primarily focused on document files and encrypted files.
Several encrypted files were discovered:

- Holiday Image – Encrypted Image
- Mariobrostheme.wav – Password hidden in audio
- Teamviewermanual – Encrypted File
- ImportantThings - Encrypted File

FINDINGS

After processing the Stockholm disk, the disk was analyzed with various forensic tools.

Document/Files: A few documents were discovered that may be used as proof. Nathan Spire's paperwork had various suspicious files. Nathan had some files in his work documents that contained crucial information. Nathan was caught with two documents that proved he was running a scam. Nathan's scheme was detailed in the Process.docx document he found in his work papers. The operation was carried out, according to the paper, using an application named Zoiper, and the main goal was to acquire access to the victim's system. It demonstrates the procedure; the user will require TeamViewer and will be charged by providing a photo of a gift card.



WordPad does not support all of the features of this document's format. Some content might be missing or displayed improperly.

Microsoft Support Process

Once you answer a call on Zoiper, the main aim is to gain access to the user's system. It will be important to get the caller to download TeamViewer so you can to show them the bad hackers on their computer.

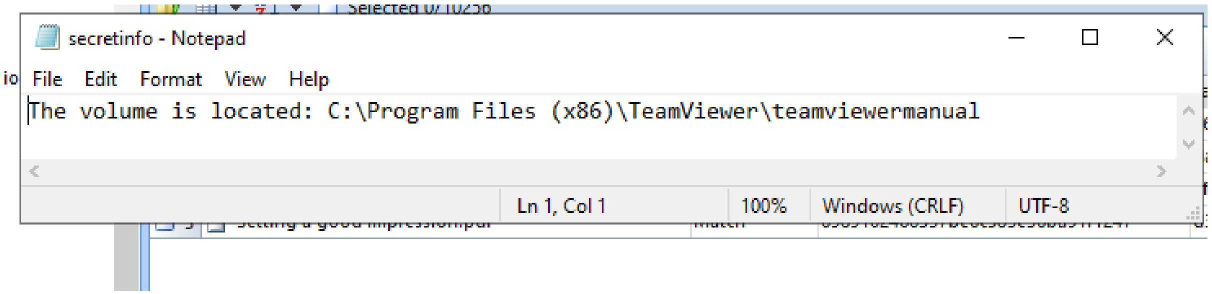
A good trick is to open the event viewer and show the customer all the errors. Explain to them that these errors are caused by malware the hackers have installed on their machine.

Most non-technical users will not understand what the event viewer is. You can then prompt the user to pay for a one-time repair fee and proceed to install anti-virus on their system.

The customer will need to pay for the service by sending a picture of a gift card.

Figure 1: Process.docx

Another file found was the Secretino.txt file. It was suspicious and it contained a note stating the volume of where a file is hidden.



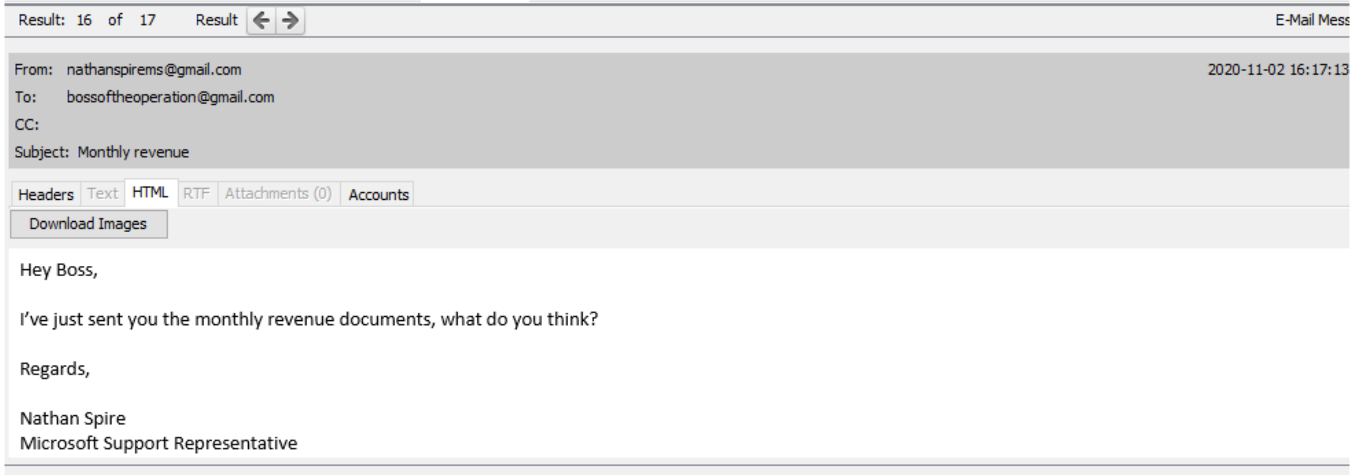
```
The volume is located: C:\Program Files (x86)\TeamViewer\teamviewermanual
```

Figure 2: SecretInfo.txt

Other files were found later on in the case which were the Victims AND Monthly Revenue excel sheets.

EMAILS: Email conversations were found after processing the case on Autopsy. Nathan Spire Email was found having a conversation with someone else and they were talking about how to carry out the scam campaign. An Email of Nathan talking to one of his victims is also found the case

DATE	SENDER	RECEIVER	DETAILS
02/11/2020	nathanspirems@gmail.com	bossoftheoperation@gmail.com	Nathan sent an excel sheet named Monthly revenue containing the sales record of the customers (Victims) he has helped, and the amount of money collected
02/11/2020	bossoftheoperation@gmail.com	nathanspirems@gmail.com	The bossoftheopration sent a music file to Nathan to investigate. This music file contained a hidden message.
02/11/2020	nathanspirems@gmail.com	bossoftheoperation@gmail.com	Nathan sent an Email asking the boss about the Process Doc document. This is the document containing the instruction of how to carry out the operation. It was earlier sent by the bossoftheoperation
02/11/2020	Sara.hoyle.personal@gmail.com	nathanspirems@gmail.com	Sara sent an Email to Nathan to Thank him and confirm the payment by sending a giftcard.



From: nathanspirems@gmail.com 2020-11-02 16:17:13
To: bossoftheoperation@gmail.com
CC:
Subject: Monthly revenue

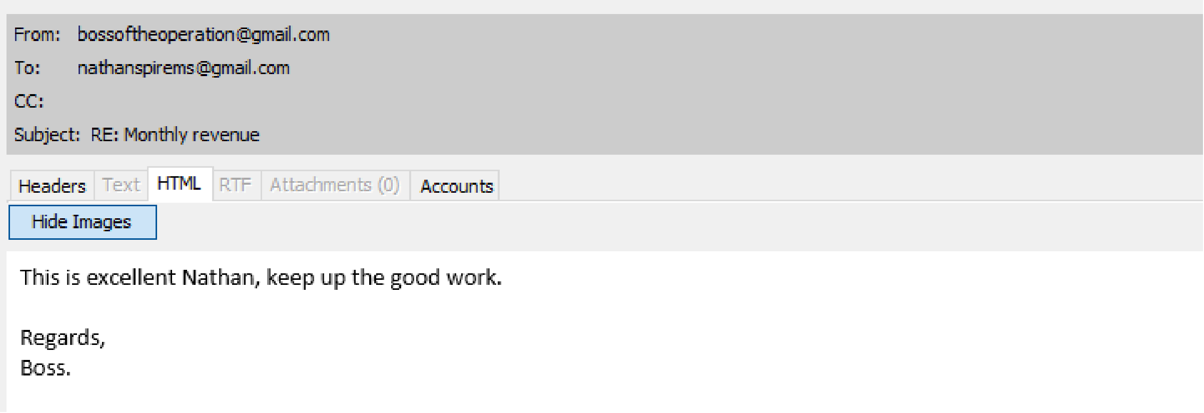
Hey Boss,

I've just sent you the monthly revenue documents, what do you think?

Regards,

Nathan Spire
Microsoft Support Representative

Figure 3: Monthly Revenue Email

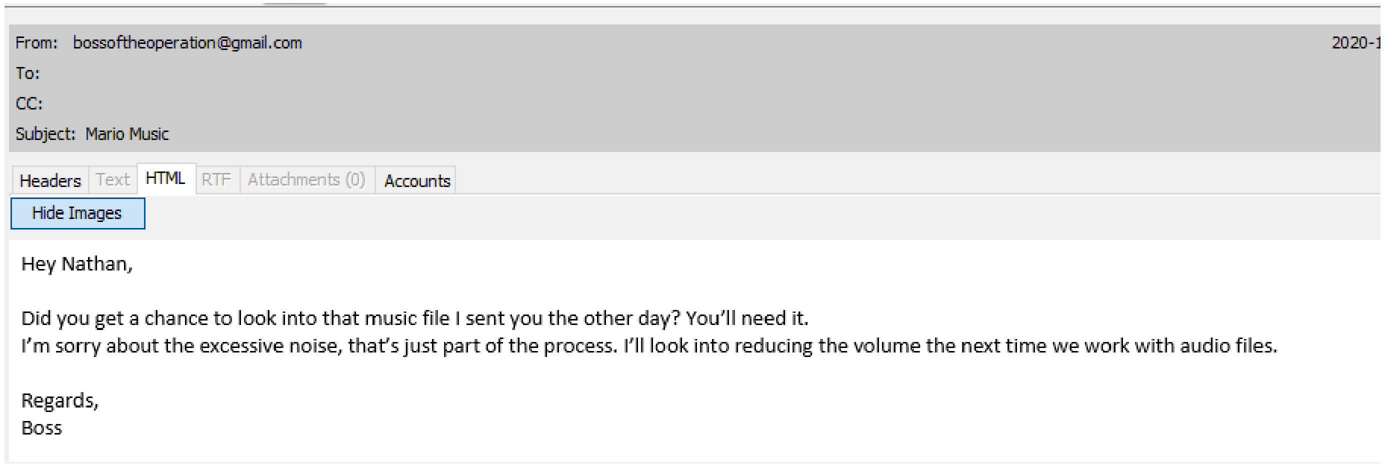


From: bossoftheoperation@gmail.com
To: nathanspirems@gmail.com
CC:
Subject: RE: Monthly revenue

This is excellent Nathan, keep up the good work.

Regards,
Boss.

Figure 4: Monthly Revenue Email Reply

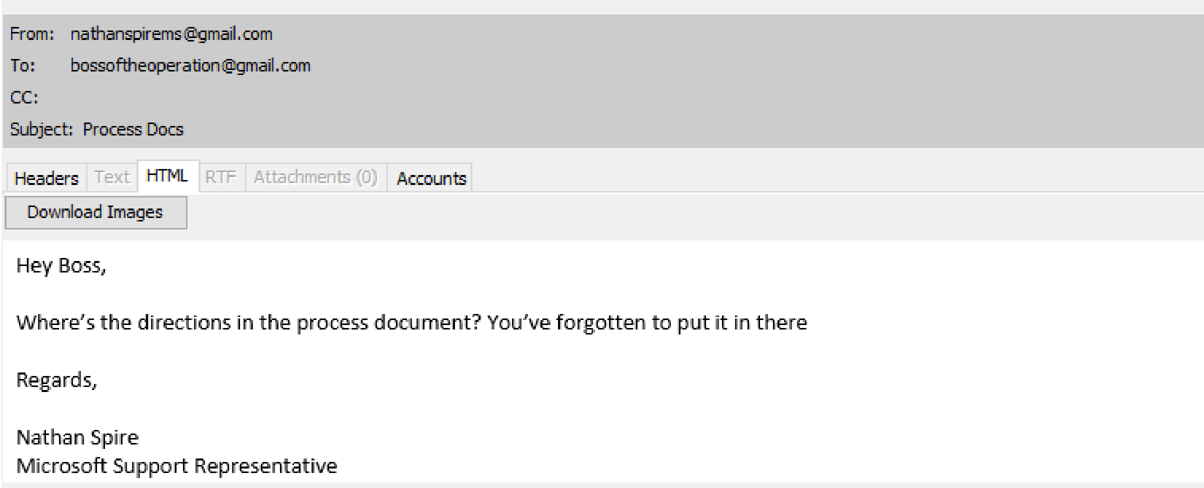

From: bossoftheoperation@gmail.com 2020-1
To:
CC:
Subject: Mario Music

Hey Nathan,

Did you get a chance to look into that music file I sent you the other day? You'll need it.
I'm sorry about the excessive noise, that's just part of the process. I'll look into reducing the volume the next time we work with audio files.

Regards,
Boss

Figure 5: Mario Music Email


From: nathanspirems@gmail.com
To: bossoftheoperation@gmail.com
CC:
Subject: Process Docs

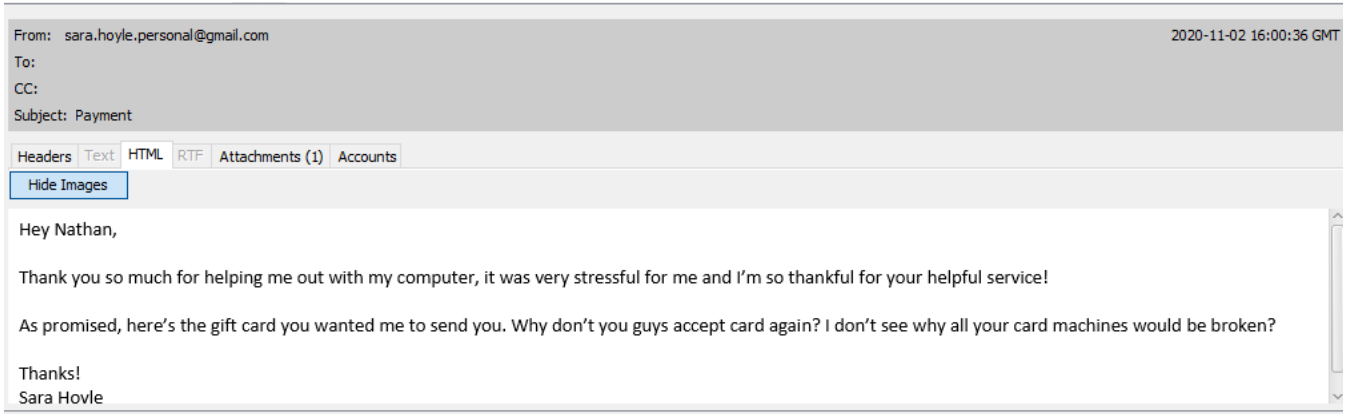
Hey Boss,

Where's the directions in the process document? You've forgotten to put it in there

Regards,

Nathan Spire
Microsoft Support Representative

Figure 6: Process Doc



From: sara.hoyle.personal@gmail.com 2020-11-02 16:00:36 GMT
To:
CC:
Subject: Payment

Hey Nathan,

Thank you so much for helping me out with my computer, it was very stressful for me and I'm so thankful for your helpful service!

As promised, here's the gift card you wanted me to send you. Why don't you guys accept card again? I don't see why all your card machines would be broken?

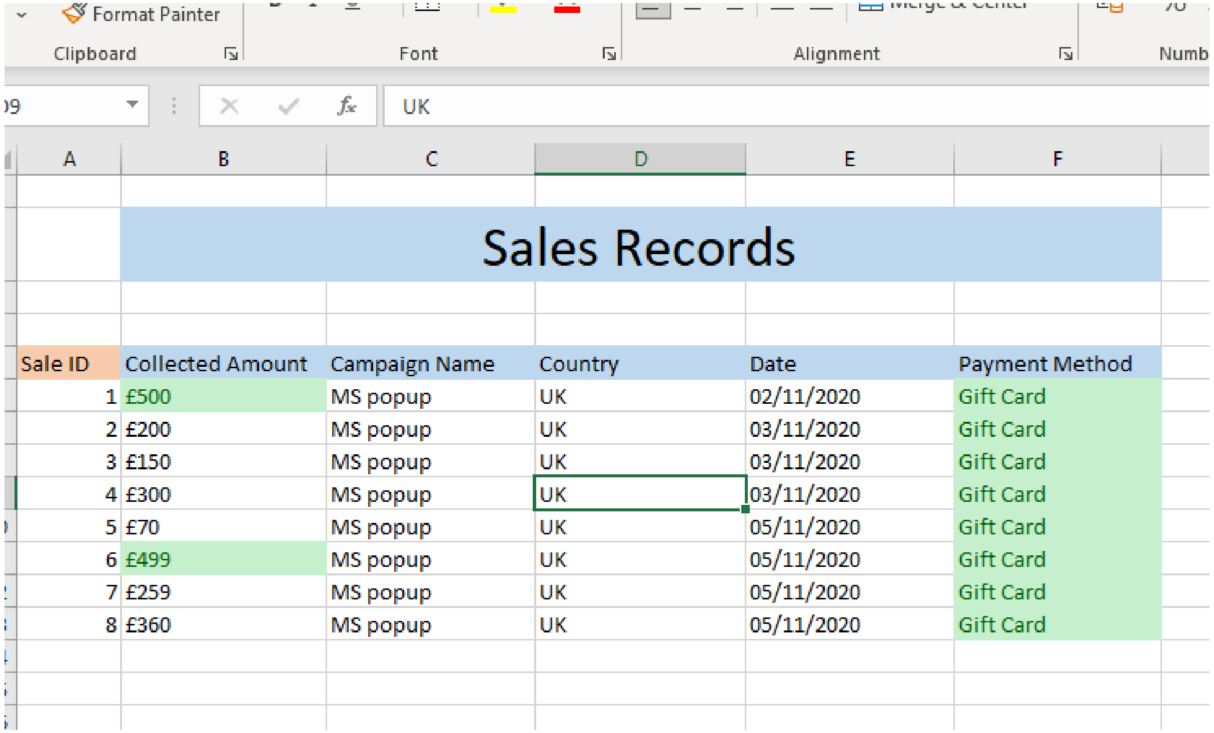
Thanks!
Sara Hoyle

Figure 7: Payment Email

ENCRYPTED FILES: There were several encryption and hidden messages in the case. These were found using Encase and Autopsy. The Encrypted files found were:

- ImportantThings
- Teamviewermanual

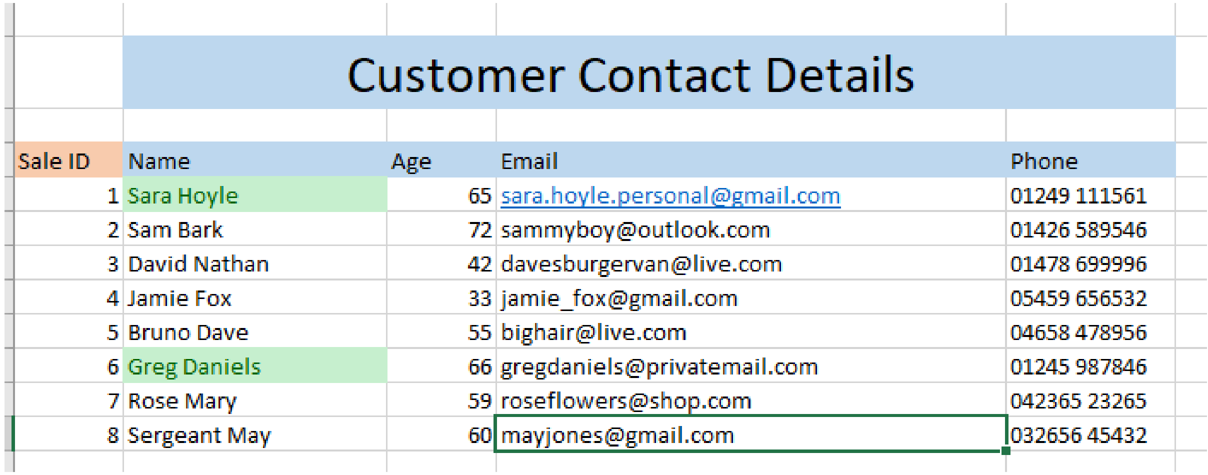
These were located by analyzing the Secret Info Text, it contained a text stating where a volume is located. These two files were further investigated, there were decrypted using VeraCrypt. Although finding the password were tasking. The password for the ImportantThings was hidden in the Mario audio file sent to Nathan "mariobrostheme.wav" it analyzed using Sonic Visualizer and it contained hidden password: **'STAPE',** this password was used to decrypt the ImportantThings volume and after decrypting it two files were found which were the **Holiday.txt** file and the **Monthly Revenue** Excel Spreadsheet. The holiday.txt contained a password; **'ArrowsAllAround'** and the Monthly Revenue contained sales information that was carried out by Nathan and how much he made. The holiday.txt password was used to open the holiday Image using Openstego and it extracted a password.txt file, this password text file contained the password 'MONEYMAKER' which was used to decrypt the Teamviewermanual using VeraCrypt, after decrypting it an excel sheet named **'Victims'** was found, it contained the contact details of the victims Nathan claimed to be helping.



Sales Records

Sale ID	Collected Amount	Campaign Name	Country	Date	Payment Method
1	£500	MS popup	UK	02/11/2020	Gift Card
2	£200	MS popup	UK	03/11/2020	Gift Card
3	£150	MS popup	UK	03/11/2020	Gift Card
4	£300	MS popup	UK	03/11/2020	Gift Card
5	£70	MS popup	UK	05/11/2020	Gift Card
6	£499	MS popup	UK	05/11/2020	Gift Card
7	£259	MS popup	UK	05/11/2020	Gift Card
8	£360	MS popup	UK	05/11/2020	Gift Card

Figure 8: Monthly Revenue Excel Sheet



Customer Contact Details

Sale ID	Name	Age	Email	Phone
1	Sara Hoyle	65	sara.hoyle.personal@gmail.com	01249 111561
2	Sam Bark	72	sammyboy@outlook.com	01426 589546
3	David Nathan	42	davesburgervan@live.com	01478 699996
4	Jamie Fox	33	jamie_fox@gmail.com	05459 656532
5	Bruno Dave	55	bighair@live.com	04658 478956
6	Greg Daniels	66	gregdaniels@privatemail.com	01245 987846
7	Rose Mary	59	roseflowers@shop.com	042365 23265
8	Sergeant May	60	mayjones@gmail.com	032656 45432

Figure 9: Victims Contact Details

SUMMARY AND OPINION

Following an examination of the case and the sequence of events, Nathan and the bossoftheoperation were involved in defrauding individuals by giving help in return for giftcard payments and committing a severe crime by acquiring access to the user's system.
The case, in my opinion, is genuine; it has proven that Nathan Spire is guilty and implicated in the claimed crime. Nathan and his accomplice have intruded on people's private, and they might face charges of invasion of privacy and fraud. After processing, the data and information obtained on the forensic picture disc proved to be beneficial. Nathan's attempt to generate money and invade privacy took time to plan, and he and his accomplice deliberated long and hard before carrying out the task of encrypting files and concealing information, but the evidence acquired demonstrates that they are unquestionably guilty.

Appendix A: Forensic Image Analysis

Student Number: 20044248

Section A: Findings
The following evidence items were found:

Evidence item number	**Full Provenance to include the following fields only (marks will be deducted if you include fewer or additional fields);**	**Method of discovery**	**Description of item**	**Significance to case**
1	**Name:** Drive D **Is Deleted: No** **File Created: 05/11/2020 15:24:33 GMT** **Last Written: 05/11/2020 15:24:33 GMT** **Last Accessed: 05/11/2020 15:24:33 GMT** **Logical Size: 552** **Physical Sector: 2,506,902** **Full path (Encase): Stock_H Case.E01/unititled/D (Encase)** **Hash: Not Calculated**	Loaded on the Encase software and Autopsy	Drive Partition	Contains all the evidence relevant to the case
2	**Name: nathanspireMS@gmail.com.ost** **Is Deleted: No** **File Created: 05/11/2020 15:38:40 GMT** **Last Written: 05/11/2020 11:40:01 GMT** **Last Accessed: 05/11/2020 15:38:40** **Logical Size: 16,818,176** **Physical Sector: 3,702,424** **Full path (Autopsy): /img_Stockholm Case Image.E01/vol_vol6/Users/Nathan Spire/AppData/Local/Microsoft/Outlook/nathanspireMS@gmail.com.ost**	Found using Encase but was in .ost, further broke down to discovery several Email Conversation after using Autopsy	**File, Archive:** Outlook email .ost, outlook storage file contains Email conversation which can be used as supporting evidence.	Contains Email conversations of Nathan Spire and another suspect (bossoftheoperation) talking about how to carry out attacks to their victims.

	Hash: MD5- 23db180e291145dbf12fdd06a6caff46 **SHA-256: 69cb74740f0f5225fa090da456a72bb44c9485c571ace4c64fdda06fa1d78d15**			
3	**Name: mariobrostheme.wav** **Is Deleted: No** **File Created: 05/11/2020 15:47:53 GMT** **Last Written: 02/11/2020 14:20:55 GMT** **Last Accessed: 05/11/2020 15:47:59 GMT** **Logical Size: 14,494,696** **Physical Sector: 5,649,960** **Full path (Encase): Stockholm_Case/untitled/D/Users/Nathan Spire/Music/Mario/mariobrostheme.wav** **Hash: MD5- 622f70478dd78f54949fa08d9871c13a** **SHA-256: d402db16a5d9f72be7bb36c58dcf0c9429104cfdaa0f37d06b3a69017fdb44a1**	Discovered after finding a conversation between Nathan and his accomplice talking about a Mario audio file, furthermore, checked Nathan Spires Music file in Encase and found a .wav extension which may contain a compressed audio.	**Audio File:** .wav audio file containing a hidden password in the text	After analysing the audio file using various audio tools such as Sonic Visualiser and Audacity a password text was found. **Password Text: ‘STAPLE’**
4	**Name: ImportantThings** **Is Deleted: No** **File Created: 05/11/2020 15:30:54 GMT** **Last Written: 02/11/2020 16:42:51 GMT** **Last Accessed: 09/11/2020 13:01:56 GMT** **Logical Size: 52,428,800** **Physical Sector: 1,906,112** **Full path (Autopsy): /img_Stockholm Case Image.E01/vol_vol6/Program Files (x86)/Windows Photo Viewer/ImportantThings** **Hash: MD5 - e3b659da3d4df978e3351ebde26388c1** **SHA-256: ce8b886c11082cdfc053276b0cafd3d1667e014d6b0192e6abc09a5c7b1ac837**	Discovered using Autopsy. File was suspected of having encrypted files and it also gave a high value entropy.	**File, Volume:** File System volume which contained encrypted files in it.	The Volume was decrypted using **VeraCrypt** the password was the one gotten from the .wav audio file although after several attempts the password wasn’t **‘STAPLE’** but **‘STAPE’**. Contains files: Holiday and Monthly Revenue excel sheet.

5	**Name: holiday.txt** **Is Deleted: Yes – Encrypted in Volume** **File Created: 02/11/2020 15:45:28 GMT** **Last Written: 02/11/2020 14:24:24 GMT** **Last Accessed: 09/11/2020** **Logical Size: 15** **Physical Sector:** **Full path:** **Hash:**	Located in the encrypted volume **'ImportantThings'.** After decrypting the volume, the holiday text file was found	**Text File**	Text file containing a password text **'ArrowsAllAround'** which is used to unlock the stego holiday image.
6	**Name: Holiday.png** **Is Deleted: No** **File Created: 05/11/2020 15:46:42 GMT** **Last Written: 02/11/2020 15:24:32** **Last Accessed: 05/11/2020 15:46:44 GMT** **Logical Size: 1,583,803** **Physical Sector: 5.066,880** **Full path (Encase): Stockholm_Case/untitled/D/Users/Nathan Spire/Documents/Travel/Holiday.png** **Hash: MD5- 0fe807ca5f47de3ef64a46d119d8cf3c** **SHA-256: 06290769697a392f72c4af4417e77a90649798b8715b702065073f8c52b32348**	Found using **Encase** in the User folder of Nathan Spire after extracting the encrypted volume ImportanThings Using **VeraCrypyt** and then finding a **holiday** text file which should be linked to the holiday image in Nathan's Travel folder	**Image:** Stego PNG Image of the Stockholm sent by the bossoftheoperation	Contains hidden text that was encrypted using **openstego**. After getting password from the ImportantThings volume. **Password for Stego Image: 'ArrowsAllAround'** Evidence was found after extracting the image using openstego. A password text file was extracted which contained the text **'MONEYMAKER'**

7	**Name: processdoc.docx:secretinfo.txt** **Is Deleted: No** **File Created: 05/11/2020 15:46:49 GMT** **Last Written: 09/11/2020 12:43:34 GMT** **Last Accessed: 09/11/2020 12:46:06 GMT** **Logical Size: 73** **Physical Sector: 2,525,886** **Full path (Autopsy): /img_Stockholm Case Image.E01/vol_vol6/Users/Nathan Spire/Documents/Work/processdoc.docx:secretinfo.txt** **Hash: MD5- 4e52e1e83b6ac8c737125c38b3af027d** **SHA-256: 8eeada5d271c15c505cd4ee2bafc5caa4db4381c9792d9ae00fb795b08d4bd54**	Discovered in Nathan Spire's **work** folder in the documents	**Plain Text:** Text file containing secret information according to the name of the text file.	Contains information stating the location of a volume named **teamviewermanual** that has hidden data
8	**Name: teamviewermanual** **Is Deleted: No** **File Created: 05/11/2020 15:30:07 GMT** **Last Written: 02/11/2020 16:43:40** **Last Accessed: 09/11/2020 13:01:43** **Logical Size: 52,428,800** **Physical Sector: 1,673,584** **Full path (Encase): Stockholm_Case/untitled/D/Program Files(x86)/TeamViewer/teamviewermanual** **Hash: MD5- 1639ac2f2eaaea369d9bf8d2248d52e2** **SHA-256: 12ba4206cea81421fe94b65433b7efee62ab07f08920ee07b1ac5b77df5f232b**	Located after discovering information about the path in a secret text file from Nathan's documents	**File, Volume:** File System Volume which contains information. Volume is encrypted	Volume was decrypted using VeraCrypt using the password gotten from the previous text file **'MONEYMAKER'** and an excel sheet **(Victims.xlsx)** containing the Victims contact details was found.
9	**Name: process.docx** **Is Deleted: No** **File Created: 05/11/2020 15:46:49 GMT** **Last Written: 09/11/2020 12:43:34 GMT** **Last Accessed: 09/11/2020 12:46:06 GMT** **Logical Size: 155,885** **Physical Sector: 5,744,432** **Full path (Encase): Stockholm_Case/unititled/D/Users/Nathan Spire/Documents/Work/processdoc.docx** **Hash: MD5- 6cc50e396e5506aa285d7d9a8baddc59** **SHA-256: e867f0de4dfade6f02725cd57fbe2c60954960030256e9c976a59acf7555923b**	Found in Nathan Spire documents	**Word Document:** Document file containing information about an application called Zoiper	Word File containing a description of how to use an application called Zoiper to call customers and secretly gain access into their system and helping them but collecting payment in gift cards.
10	**Name: Zoiper5_installer_v5.4.9.exe** **Is Deleted: No** **File Created: 05/11/2020 15:47:17 GMT** **Last Written: 02/11/2020 13:16:57 GMT** **Last Accessed: 05/11/2020 15:47:50 GMT** **Logical Size: 175,750,744** **Physical Sector: 5,301,104** **Full path: Stockholm_Case/untitled/D/Users/Nathan Spire/Downloads/Zoiper5_installer_v5.4.9.exe** **Hash: MD5- 6d6b8b35b8a510695796c3457002f95d**	Located in Nathan's downloaded files	**Exe Application:** Zoiper application used to call customers	Nathan downloaded this application which is evident he used it to communicate with customers and carry out unlawful acts.

	SHA-256: **4f1d9cf6d4059ab6414f9724081f60f53741a4a45cc7cf7dbe00c49a80f75bb8**			
11	**Name: monthlyrevenue.xlsx** **Is Deleted: NO, Encrypted** **File Created: 02/11/2020 15:45:28 GMT** **Last Written: 02/11/2020 14:36:54 GMT** **Last Accessed: 09/11/2020** **Logical Size: 10,677** **Physical Sector:** **Full path:** **Hash:**	Found after decrypting the ImportantThings file volume found in Nathan's Computer	**Excel Spreadsheet:** Excel file contating the monthly revenue and the amount of money customers paid.	This file contains the amount of money Nathan has collected from his victims through paying with gift cards.
12	**Name: Victims.xlsx** **Is Deleted: No, Encrypted** **File Created: 02/11/2020 15:44:08 GMT** **Last Written: 02/11/2020 14:52:20 GMT** **Last Accessed:** **Logical Size:** **Physical Sector:** **Full path:** **Hash:**	Found after decrypting the Teamviewermanual file volume found in Nathan's Computer	**Excel Spreadsheet:** Excel spreadsheet containing the name of the victims and their contact details.	This spreadsheet was encrypted and after decrypting the volume the file contained the victims' contact details.
13	**Name: giftcard.jpg** **Is Deleted: No** **File Created: 05/11/2020 15:38:40 GMT** **Last Written: 05/11/2020 11:40:01 GMT** **Last Accessed: 05/11/2020 15:28:45 GMT** **Logical Size: 16,818,176** **Physical Sector: 3,702,424** **Full path: /img_Stockholm Case Image.E01/vol_vol6/Users/Nathan Spire/AppData/Local/Microsoft/Outlook/nathanspireMS@gmail.com.ost/giftcard.jpg** **Hash: MD5- 23db180e291145dbf12fdd06a6caff46** **SHA-256:** **69cb74740f0f5225fa090da456a72bb44c9485c571ace4c64fdda06fa1d78d15**	Located in one of the email conversations from Nathan and Sara Hoyle	**Image:** Image of gift card of $500	This gift card was sent by Sara Hoyle, one of Nathan's Victims. It was sent as a payment method to Nathan

Appendix B: Evidence Map

Key Details

Document/File	🟨
Passwords	⬛
Veracrypt	🟥
Stegged Images	🟪
Emails	🟩
Encrypted Files	🟦
Audio	🟥

Emails

Emails to and from:

nathanspirems@gmail.com (Suspect)

bossoftheoperation@gmail.com (Nathan's partner)

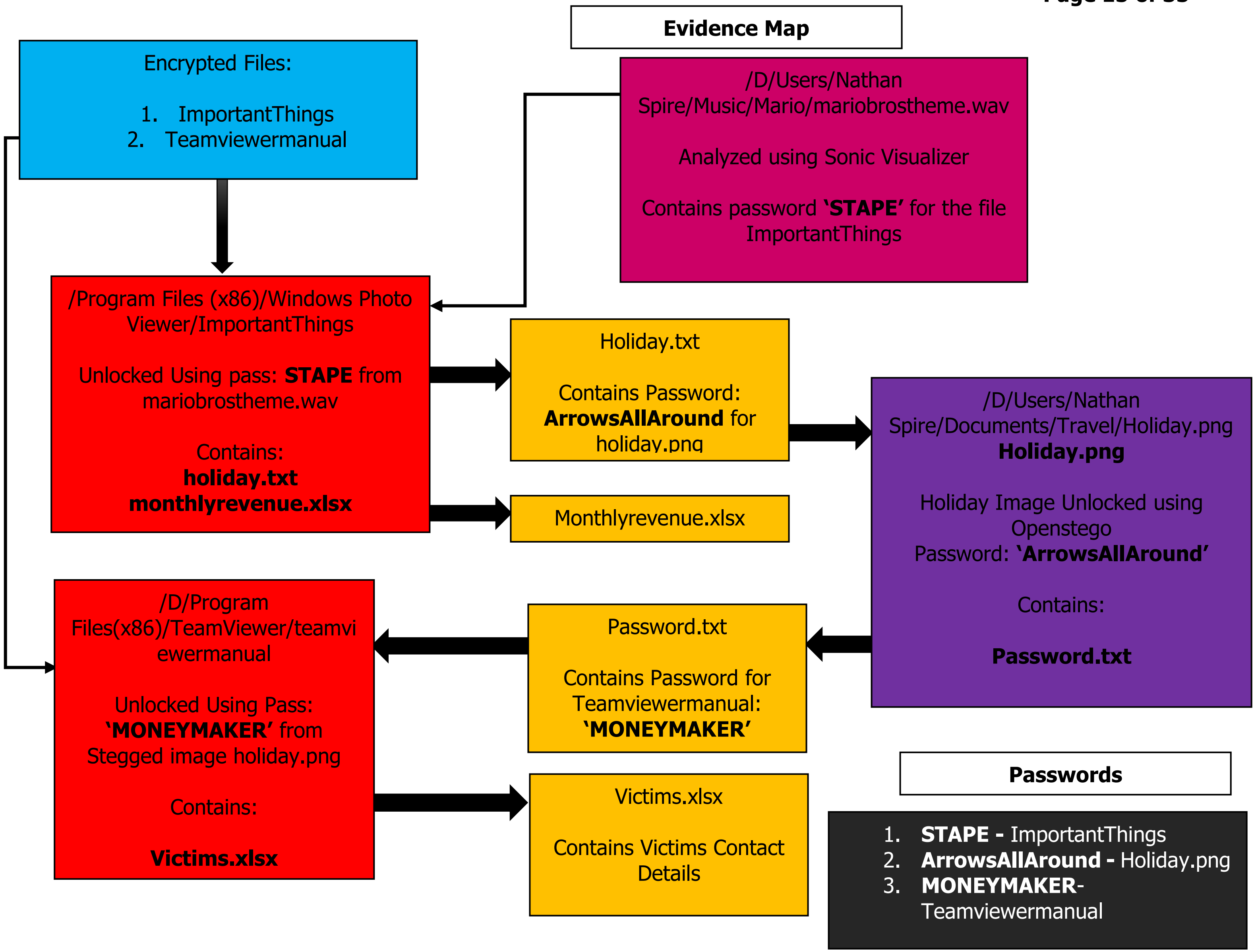
Sara.hoyle.personal@gmail.com (Nathan's Victim)

Email Attachments:

Holiday.png

Mariobrostheme.wav

Giftcard.jpg



Evidence Map

Encrypted Files:

1. ImportantThings
2. Teamviewermanual

/D/Users/Nathan Spire/Music/Mario/mariobrostheme.wav

Analyzed using Sonic Visualizer

Contains password **'STAPE'** for the file ImportantThings

/Program Files (x86)/Windows Photo Viewer/ImportantThings

Unlocked Using pass: **STAPE** from mariobrostheme.wav

Contains:
holiday.txt
monthlyrevenue.xlsx

Holiday.txt

Contains Password: **ArrowsAllAround** for holiday.png

Monthlyrevenue.xlsx

/D/Users/Nathan Spire/Documents/Travel/Holiday.png
Holiday.png

Holiday Image Unlocked using Openstego
Password: **'ArrowsAllAround'**

Contains:

Password.txt

/D/Program Files(x86)/TeamViewer/teamviewermanual

Unlocked Using Pass: **'MONEYMAKER'** from Stegged image holiday.png

Contains:

Victims.xlsx

Password.txt

Contains Password for Teamviewermanual: **'MONEYMAKER'**

Victims.xlsx

Contains Victims Contact Details

Passwords

1. **STAPE -** ImportantThings
2. **ArrowsAllAround -** Holiday.png
3. **MONEYMAKER-** Teamviewermanual

Appendix C: Contemporaneous Notes

Examiner	Hamza Wakili	Exam commenced	09/05/2022 13:56:34 BST
Other relevant information		Software used, versions and licensing	Encase 7, Autopsy 4.19, VeraCrypt, Sonic Visualiser and Openstego

Action	Done?	Date	Time	Notes
Load case & verify image	YES	11/05/2022	00:54:07 BST	▪ Loaded the Stockholm Case Image.E01 File on Encase 7 ▪ Created a case named Stockholm_Case ▪ Encase Verified the Case ▪ Thoroughly checked and found images in the case See Figure 1 and 2
Load Case into second forensic tool for dual verification of 2 key artefacts	YES	11/05/2022	01:01:32 BST	▪ Loaded the Stockholm Case Image.E01 file on another verification tool called **Autopsy** ▪ Verified the case on Autopsy by comparing hashes ▪ Found the similar evidence on Autopsy See Figure 3

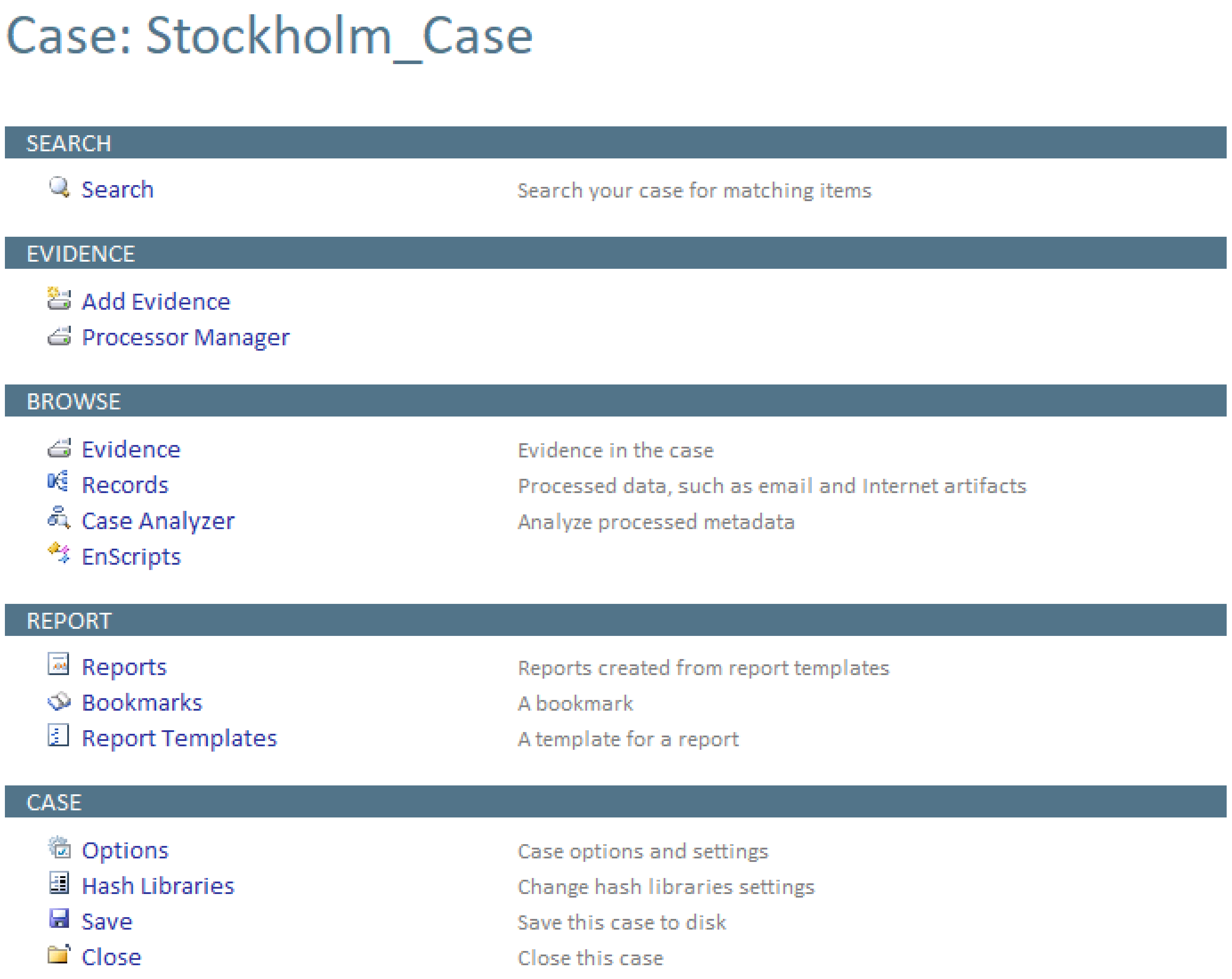
Action	Done?	Date	Time	Notes
Recover lost folders (FAT16 & 32).	YES	11/05/2022	01:15:49 BST	▪ Recovered lost folders, NTFS, and FAT 32
Mount archives; zip, thumbs.db, etc	YES	11/05/2022	01:02:41 BST	▪ Found mounted archives after using the evidence processor ▪ Found recovered archives See Figure 4
File signature analysis, compute hash values	YES	11/05/2022	01:40:33 BST	▪ File signature was noted by the Encase software ▪ Viewed and verified file signature e.g., Alias, Bad, Match, Unknown and !Bad ▪ Hash values of the case were displayed in MD5 and SHA 1 ▪ Files were shown in MD5 and SHA-256 hashes See figure 5
Perform data carving	YES	11/05/2020	03:45:41 BST	▪ Performed data carving by using the file carver module ▪ Not much relevant information ▪ Slack space and unallocated spaces were found in the disk See Figure 6
Retrieve operating system information, accounts information, software, timezone information etc).	NO	-	-	▪ No registry information on the disk
Timeline analysis- note date of last activity on the computer.	NO	-	-	▪ No registry information on the disk

Action	Done?	Date	Time	Notes
Recover Log-on passwords – use SAMInside/Ophcrack/Encase	NO	-	-	▪ No registry information on the disk
Registry analysis and Registry protected area	NO	-	-	▪ No registry information on the disk
Internet History, favourites. Other browsers?	YES	11/05/2020	05:30:30 BST	▪ Used the evidence processor to retrieve internet activities ▪ Discovered other browsers, Internet Explorer, Chrome ▪ Used the case analyzer to discover other internet activities, cookies, visited sites, bookmarks etc. ▪ History URLs, Caches and Domains were found on the case See Figure 7
Run relevant keyword searches	YES	11/05/2020	5:43:18 BST	▪ Used the evidence processor relevant keyword search module to search for words ▪ Searched for keywords in GREP or simple text options ▪ Searched for keywords **bossoftheoperation** and **payment** See Figure 8
Emails, local & web-based.	YES	10/05/2020	00:54:47 BST	▪ Used Autopsy to look for Emails ▪ Found several outlook Email conversations on Autopsy ▪ Found 14 Email messages after processing the case on Autopsy See Figure 9

Action	Done?	Date	Time	Notes
IM clients	YES	09/05/2020	14:47:07 BST	▪ Suspected IM conversation on Zoiper Application ▪ No Recovered IM Parser on Encase ▪ Found 3 IM conversation accounts on Autopsy 1. nathanspirems@gmail.com (Suspect) 2. bossoftheoperation@gmail.com (Nathan's partner) 3. Sara.hoyle.personal@gmail.com (Nathan's Victim) See Figure 10
Examine different file types. Export doc / office & exe files; look at Meta data if required	YES	11/05/2022	03:13:40 BST	▪ Examined different file types. Wav, exe, images, and encrypted files ▪ Found installed exe applications – Zoiper5 ▪ Exported audio files, Stego Images, and files with high Entropy values (Encrypted Files) See Figure 11
Clean-up utilities. Check log files	NO	-	-	▪ No log files due to lack of registry recovery
Encryption, Steg ,	YES	11/05/2022	01:05:08 BST	▪ Examined the case on Encase and found encrypted audio file and Stego Image which are: 1. Holiday.png 2. Mariobrostheme.wav ▪ Found suspected encryption by using Autopsy ▪ Files with high value entropy were found, they were:

Action	Done?	Date	Time	Notes
				1. ImportantThings 2. Teamviewermanual - Stego images were extracted using Openstego, audio files were analyzed with sonic visualiser and encrypted files were decrypted using VeraCrypt See Figure 12, 13 and 14
Link files	YES	11/05/2022	02:55:21 BST	- Found Link files after using the Encase Link parser - Founded several linked files See Figure 15 and 16
Print artefacts	YES	17/05/2022	01:55:30 BST	- Found artifacts after processing the windows artifact parser - Discovered Indx and MFT artifacts See Figure 17
CD/DVD burning apps; check log files	NO	-	-	- No log files

Additional Notes:



Case: Stockholm_Case

SEARCH

Search	Search your case for matching items

EVIDENCE

- Add Evidence
- Processor Manager

BROWSE

Evidence	Evidence in the case
Records	Processed data, such as email and Internet artifacts
Case Analyzer	Analyze processed metadata
EnScripts	

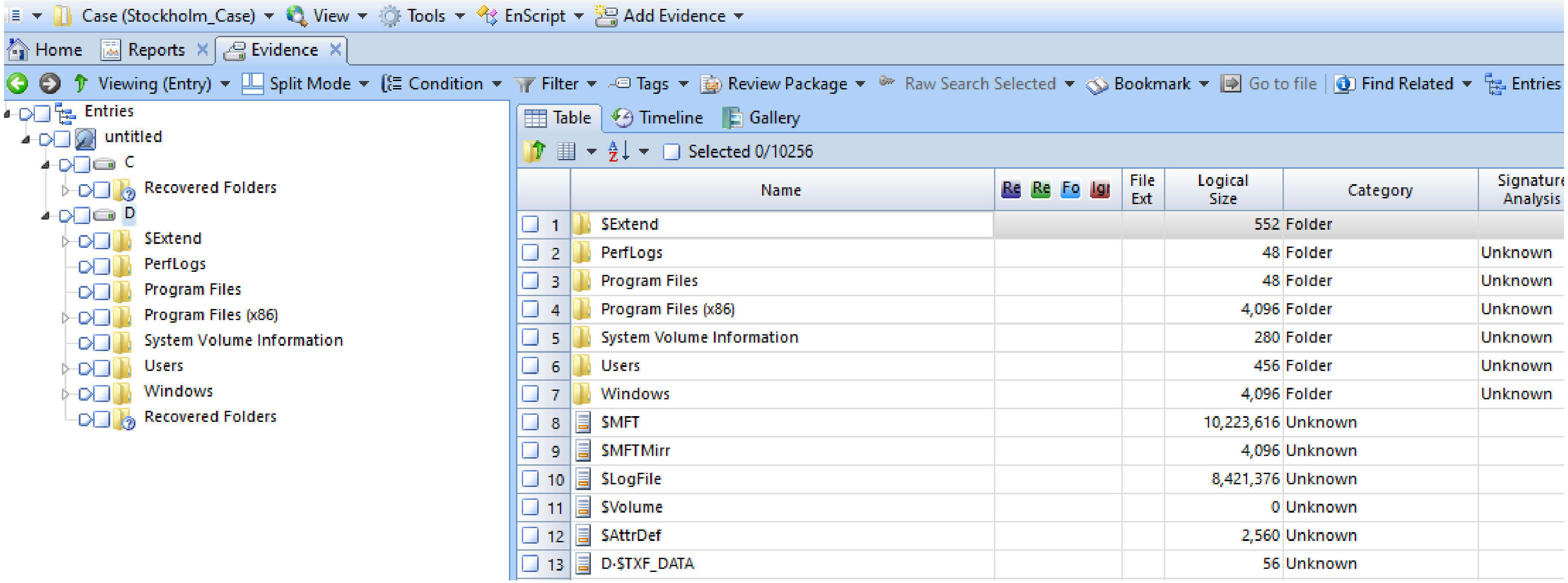
REPORT

Reports	Reports created from report templates
Bookmarks	A bookmark
Report Templates	A template for a report

CASE

Options	Case options and settings
Hash Libraries	Change hash libraries settings
Save	Save this case to disk
Close	Close this case

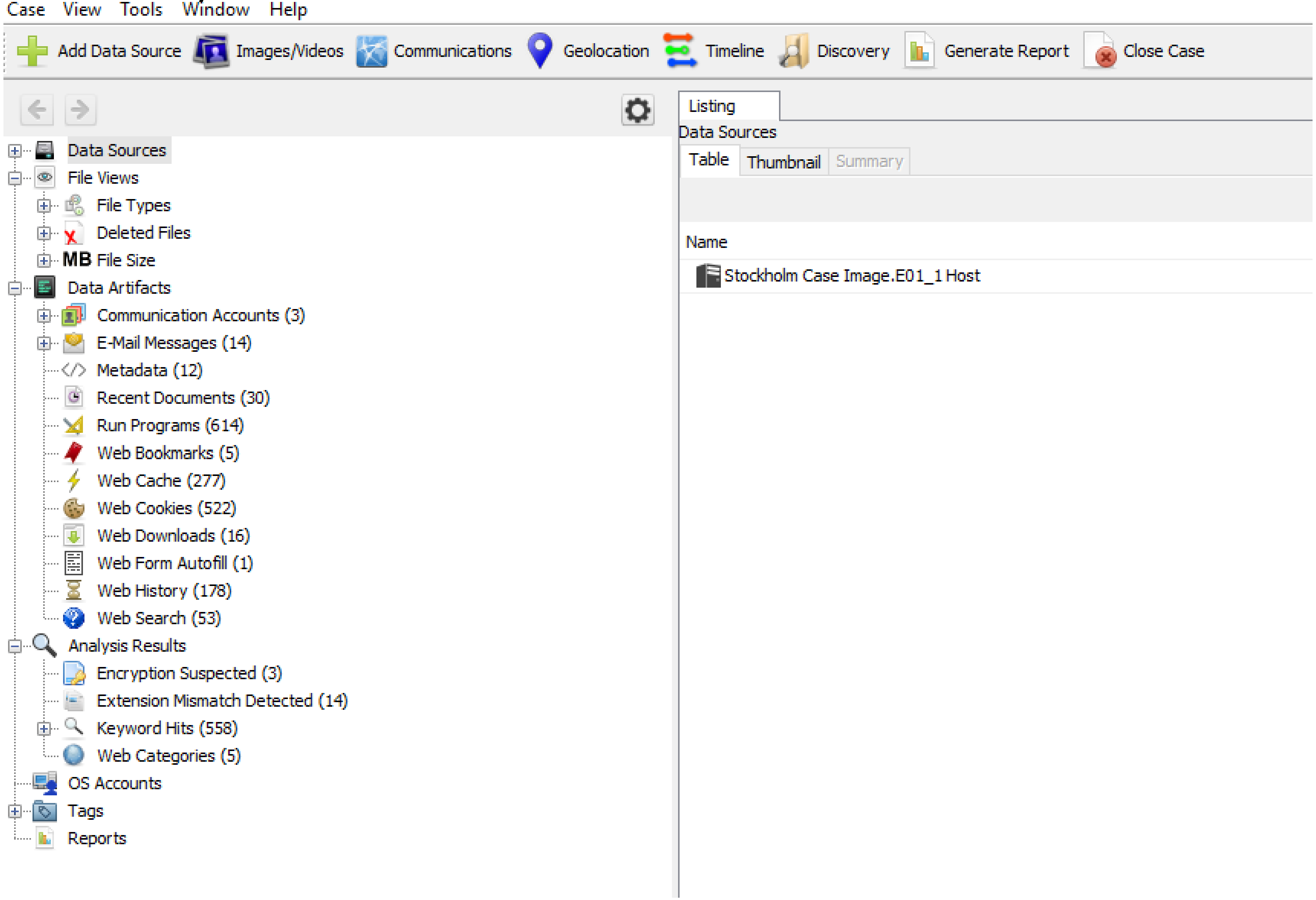
Figure 1: Encase , Creating of the Case



- Entries
  - untitled
    - C
      - Recovered Folders
    - D
      - $Extend
      - PerfLogs
      - Program Files
      - Program Files (x86)
      - System Volume Information
      - Users
      - Windows
      - Recovered Folders

	Name	Re	Re	Fo	Igı	File Ext	Logical Size	Category	Signature Analysis
1	$Extend						552	Folder	
2	PerfLogs						48	Folder	Unknown
3	Program Files						48	Folder	Unknown
4	Program Files (x86)						4,096	Folder	Unknown
5	System Volume Information						280	Folder	Unknown
6	Users						456	Folder	Unknown
7	Windows						4,096	Folder	Unknown
8	$MFT						10,223,616	Unknown	
9	$MFTMirr						4,096	Unknown	
10	$LogFile						8,421,376	Unknown	
11	$Volume						0	Unknown	
12	$AttrDef						2,560	Unknown	
13	D·$TXF_DATA						56	Unknown	

Figure 2: Encase Loading

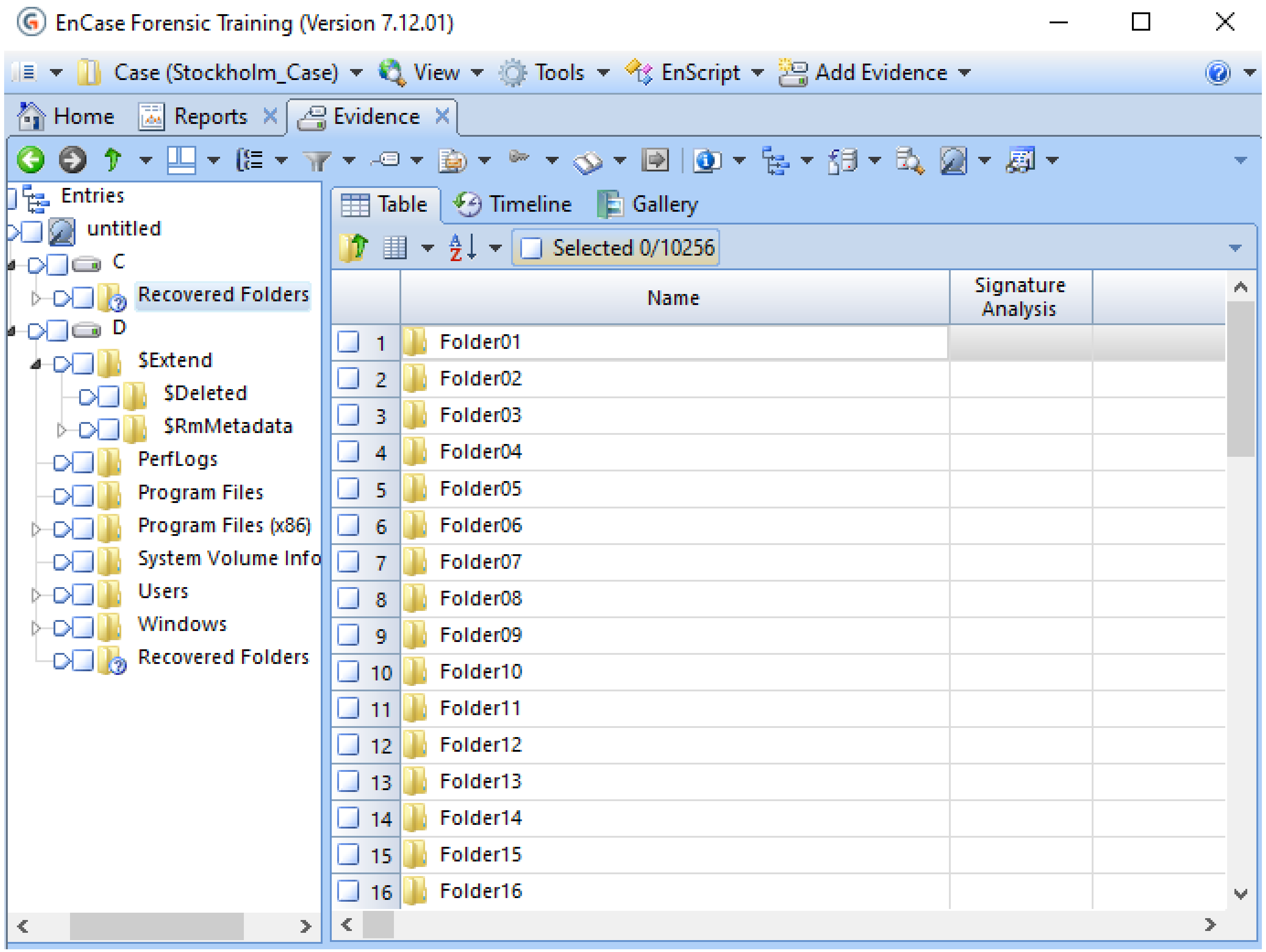


- Data Sources
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Communication Accounts (3)
  - E-Mail Messages (14)
  - Metadata (12)
  - Recent Documents (30)
  - Run Programs (614)
  - Web Bookmarks (5)
  - Web Cache (277)
  - Web Cookies (522)
  - Web Downloads (16)
  - Web Form Autofill (1)
  - Web History (178)
  - Web Search (53)
- Analysis Results
  - Encryption Suspected (3)
  - Extension Mismatch Detected (14)
  - Keyword Hits (558)
  - Web Categories (5)
- OS Accounts
- Tags
- Reports

Data Sources

Name
Stockholm Case Image.E01_1 Host

Figure 3: Autopsy Verification

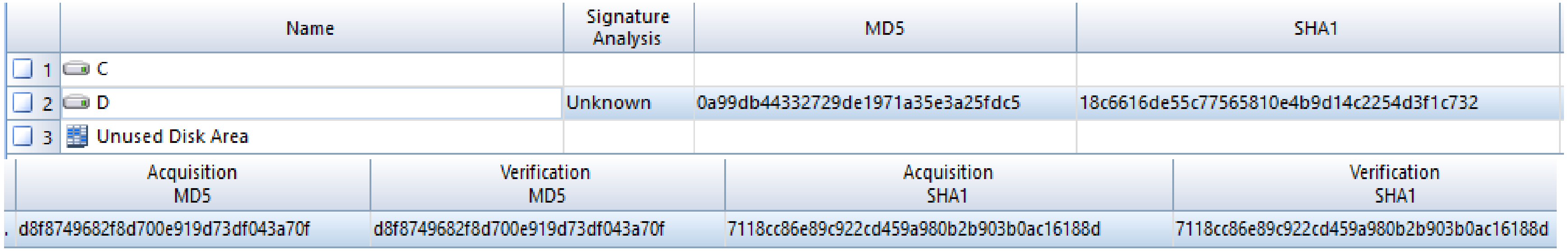


Selected 0/10256

- Entries
  - untitled
    - C
      - Recovered Folders
    - D
      - $Extend
        - $Deleted
        - $RmMetadata
      - PerfLogs
      - Program Files
      - Program Files (x86)
      - System Volume Info
      - Users
      - Windows
      - Recovered Folders

	Name	Signature Analysis
1	Folder01	
2	Folder02	
3	Folder03	
4	Folder04	
5	Folder05	
6	Folder06	
7	Folder07	
8	Folder08	
9	Folder09	
10	Folder10	
11	Folder11	
12	Folder12	
13	Folder13	
14	Folder14	
15	Folder15	
16	Folder16	

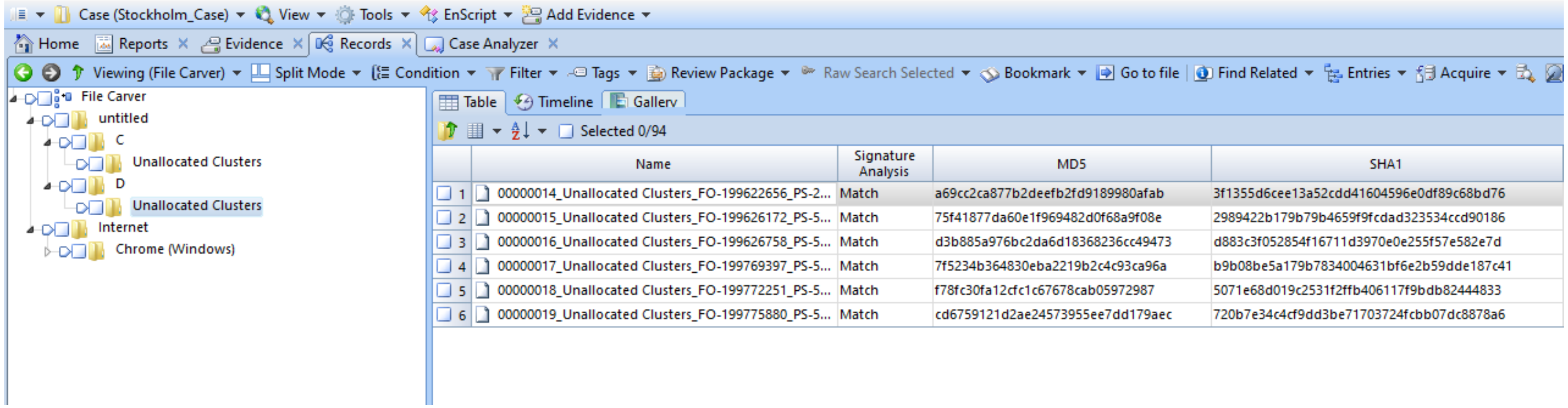
Figure 4: Recovered Folders



	Name	Signature Analysis	MD5	SHA1
□ 1	C			
□ 2	D	Unknown	0a99db44332729de1971a35e3a25fdc5	18c6616de55c77565810e4b9d14c2254d3f1c732
□ 3	Unused Disk Area			

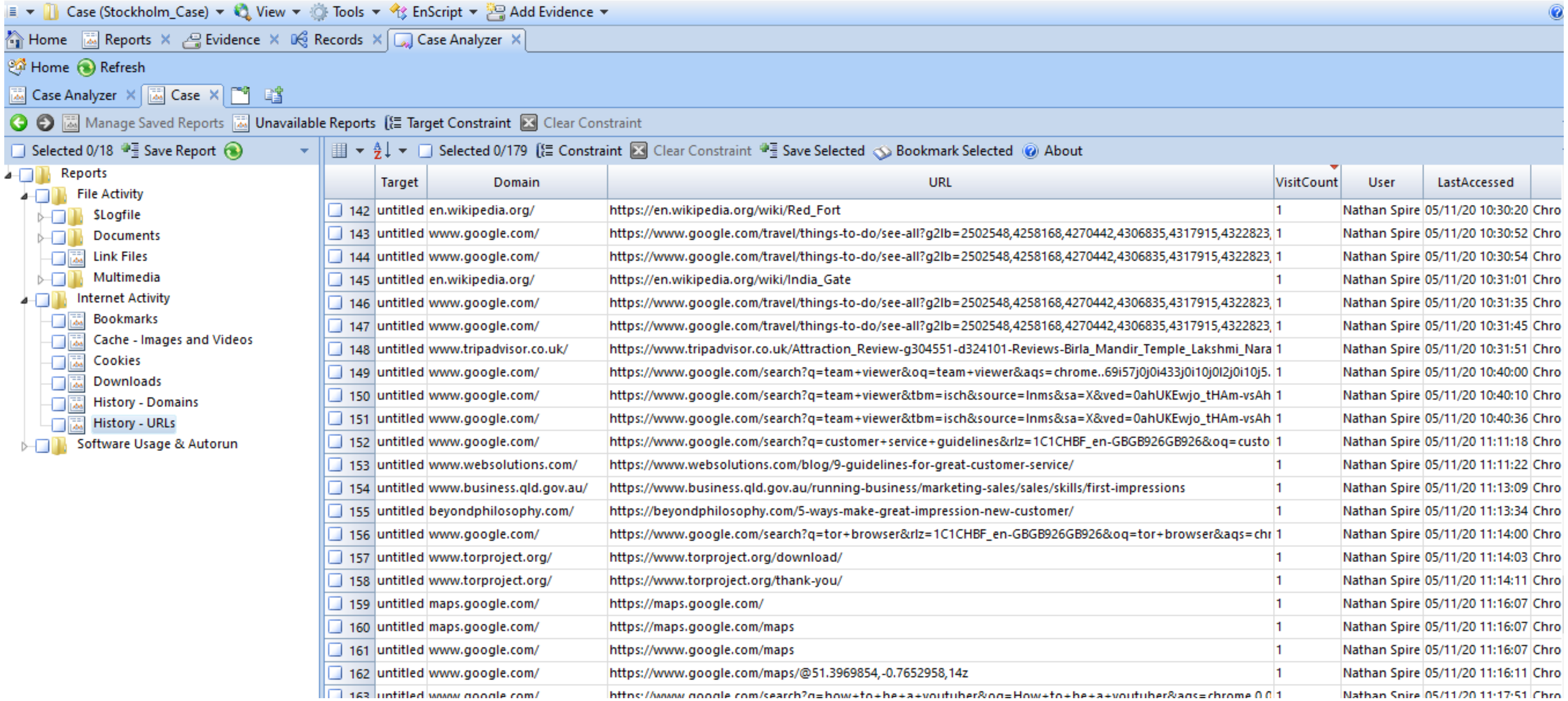
Acquisition MD5	Verification MD5	Acquisition SHA1	Verification SHA1
d8f8749682f8d700e919d73df043a70f	d8f8749682f8d700e919d73df043a70f	7118cc86e89c922cd459a980b2b903b0ac16188d	7118cc86e89c922cd459a980b2b903b0ac16188d

Figure 5: Hash and Signature Analysis



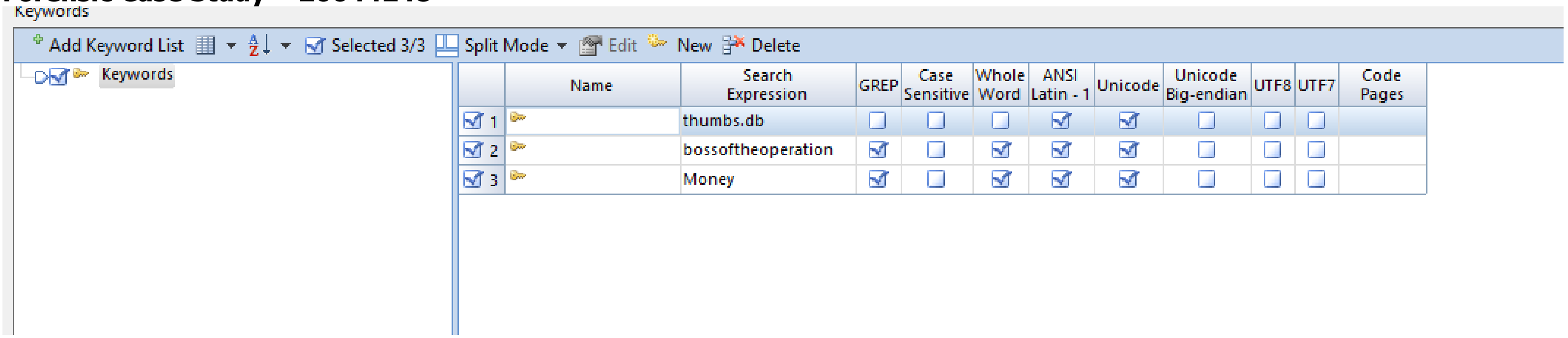
	Name	Signature Analysis	MD5	SHA1
□ 1	00000014_Unallocated Clusters_FO-199622656_PS-2...	Match	a69cc2ca877b2deefb2fd9189980afab	3f1355d6cee13a52cdd41604596e0df89c68bd76
□ 2	00000015_Unallocated Clusters_FO-199626172_PS-5...	Match	75f41877da60e1f969482d0f68a9f08e	2989422b179b79b4659f9fcdad323534ccd90186
□ 3	00000016_Unallocated Clusters_FO-199626758_PS-5...	Match	d3b885a976bc2da6d18368236cc49473	d883c3f052854f16711d3970e0e255f57e582e7d
□ 4	00000017_Unallocated Clusters_FO-199769397_PS-5...	Match	7f5234b364830eba2219b2c4c93ca96a	b9b08be5a179b7834004631bf6e2b59dde187c41
□ 5	00000018_Unallocated Clusters_FO-199772251_PS-5...	Match	f78fc30fa12cfc1c67678cab05972987	5071e68d019c2531f2ffb406117f9bdb82444833
□ 6	00000019_Unallocated Clusters_FO-199775880_PS-5...	Match	cd6759121d2ae24573955ee7dd179aec	720b7e34c4cf9dd3be71703724fcbb07dc8878a6

Figure 6: File Carving



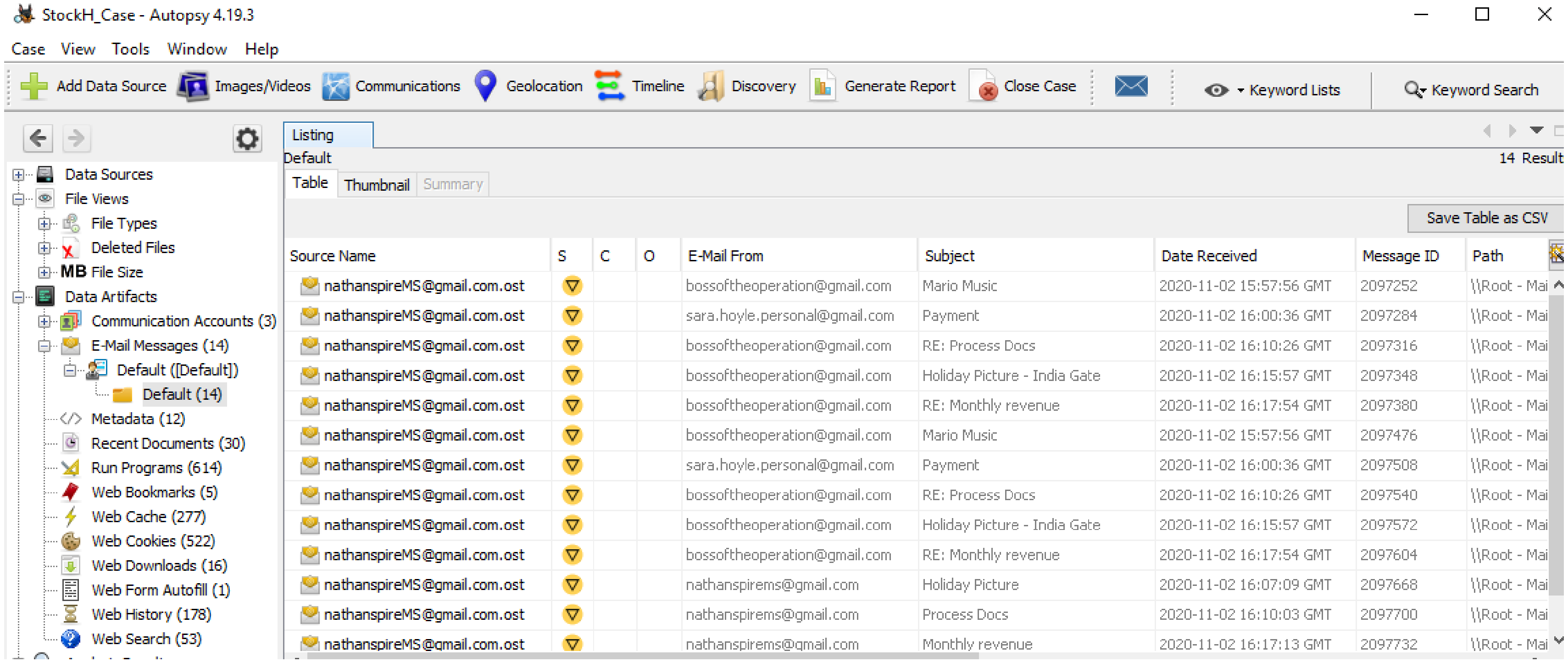
	Target	Domain	URL	VisitCount	User	LastAccessed	
□ 142	untitled	en.wikipedia.org/	https://en.wikipedia.org/wiki/Red_Fort	1	Nathan Spire	05/11/20 10:30:20	Chro
□ 143	untitled	www.google.com/	https://www.google.com/travel/things-to-do/see-all?g2lb=2502548,4258168,4270442,4306835,4317915,4322823,	1	Nathan Spire	05/11/20 10:30:52	Chro
□ 144	untitled	www.google.com/	https://www.google.com/travel/things-to-do/see-all?g2lb=2502548,4258168,4270442,4306835,4317915,4322823,	1	Nathan Spire	05/11/20 10:30:54	Chro
□ 145	untitled	en.wikipedia.org/	https://en.wikipedia.org/wiki/India_Gate	1	Nathan Spire	05/11/20 10:31:01	Chro
□ 146	untitled	www.google.com/	https://www.google.com/travel/things-to-do/see-all?g2lb=2502548,4258168,4270442,4306835,4317915,4322823,	1	Nathan Spire	05/11/20 10:31:35	Chro
□ 147	untitled	www.google.com/	https://www.google.com/travel/things-to-do/see-all?g2lb=2502548,4258168,4270442,4306835,4317915,4322823,	1	Nathan Spire	05/11/20 10:31:45	Chro
□ 148	untitled	www.tripadvisor.co.uk/	https://www.tripadvisor.co.uk/Attraction_Review-g304551-d324101-Reviews-Birla_Mandir_Temple_Lakshmi_Nara	1	Nathan Spire	05/11/20 10:31:51	Chro
□ 149	untitled	www.google.com/	https://www.google.com/search?q=team+viewer&oq=team+viewer&aqs=chrome..69i57j0j0i433j0i10j0l2j0i10j5.	1	Nathan Spire	05/11/20 10:40:00	Chro
□ 150	untitled	www.google.com/	https://www.google.com/search?q=team+viewer&tbm=isch&source=lnms&sa=X&ved=0ahUKEwjo_tHAm-vsAh	1	Nathan Spire	05/11/20 10:40:10	Chro
□ 151	untitled	www.google.com/	https://www.google.com/search?q=team+viewer&tbm=isch&source=lnms&sa=X&ved=0ahUKEwjo_tHAm-vsAh	1	Nathan Spire	05/11/20 10:40:36	Chro
□ 152	untitled	www.google.com/	https://www.google.com/search?q=customer+service+guidelines&rlz=1C1CHBF_en-GBGB926GB926&oq=custo	1	Nathan Spire	05/11/20 11:11:18	Chro
□ 153	untitled	www.websolutions.com/	https://www.websolutions.com/blog/9-guidelines-for-great-customer-service/	1	Nathan Spire	05/11/20 11:11:22	Chro
□ 154	untitled	www.business.qld.gov.au/	https://www.business.qld.gov.au/running-business/marketing-sales/sales/skills/first-impressions	1	Nathan Spire	05/11/20 11:13:09	Chro
□ 155	untitled	beyondphilosophy.com/	https://beyondphilosophy.com/5-ways-make-great-impression-new-customer/	1	Nathan Spire	05/11/20 11:13:34	Chro
□ 156	untitled	www.google.com/	https://www.google.com/search?q=tor+browser&rlz=1C1CHBF_en-GBGB926GB926&oq=tor+browser&aqs=chr	1	Nathan Spire	05/11/20 11:14:00	Chro
□ 157	untitled	www.torproject.org/	https://www.torproject.org/download/	1	Nathan Spire	05/11/20 11:14:03	Chro
□ 158	untitled	www.torproject.org/	https://www.torproject.org/thank-you/	1	Nathan Spire	05/11/20 11:14:11	Chro
□ 159	untitled	maps.google.com/	https://maps.google.com/	1	Nathan Spire	05/11/20 11:16:07	Chro
□ 160	untitled	maps.google.com/	https://maps.google.com/maps	1	Nathan Spire	05/11/20 11:16:07	Chro
□ 161	untitled	www.google.com/	https://www.google.com/maps	1	Nathan Spire	05/11/20 11:16:07	Chro
□ 162	untitled	www.google.com/	https://www.google.com/maps/@51.3969854,-0.7652958,14z	1	Nathan Spire	05/11/20 11:16:11	Chro
□ 163	untitled	www.google.com/	https://www.google.com/search?q=how+to+be+a+youtuber&oq=How+to+be+a+youtuber&aqs=chrome.0.0	1	Nathan Spire	05/11/20 11:17:51	Chro

Figure 7: Internet Artifacts



	Name	Search Expression	GREP	Case Sensitive	Whole Word	ANSI Latin - 1	Unicode	Unicode Big-endian	UTF8	UTF7	Code Pages
☑ 1		thumbs.db	□	□	□	☑	☑	□	□	□	
☑ 2		bossoftheoperation	☑	□	☑	☑	☑	□	□	□	
☑ 3		Money	☑	□	☑	☑	☑	□	□	□	

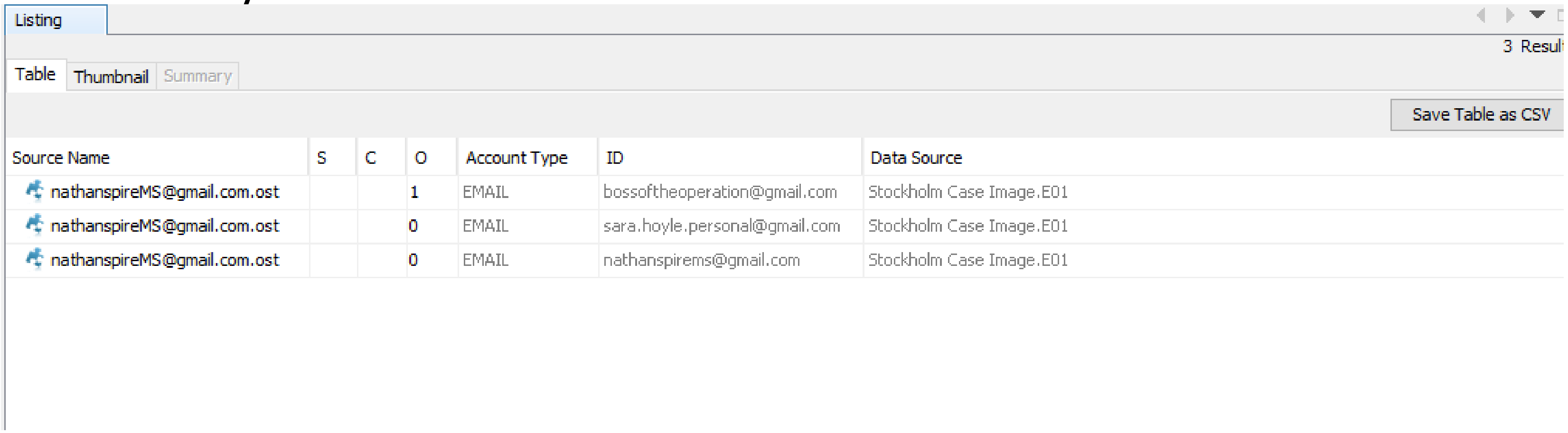
Figure 8: Keyword Searches



- Data Sources
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Communication Accounts (3)
  - E-Mail Messages (14)
    - Default ([Default])
      - Default (14)
  - Metadata (12)
  - Recent Documents (30)
  - Run Programs (614)
  - Web Bookmarks (5)
  - Web Cache (277)
  - Web Cookies (522)
  - Web Downloads (16)
  - Web Form Autofill (1)
  - Web History (178)
  - Web Search (53)

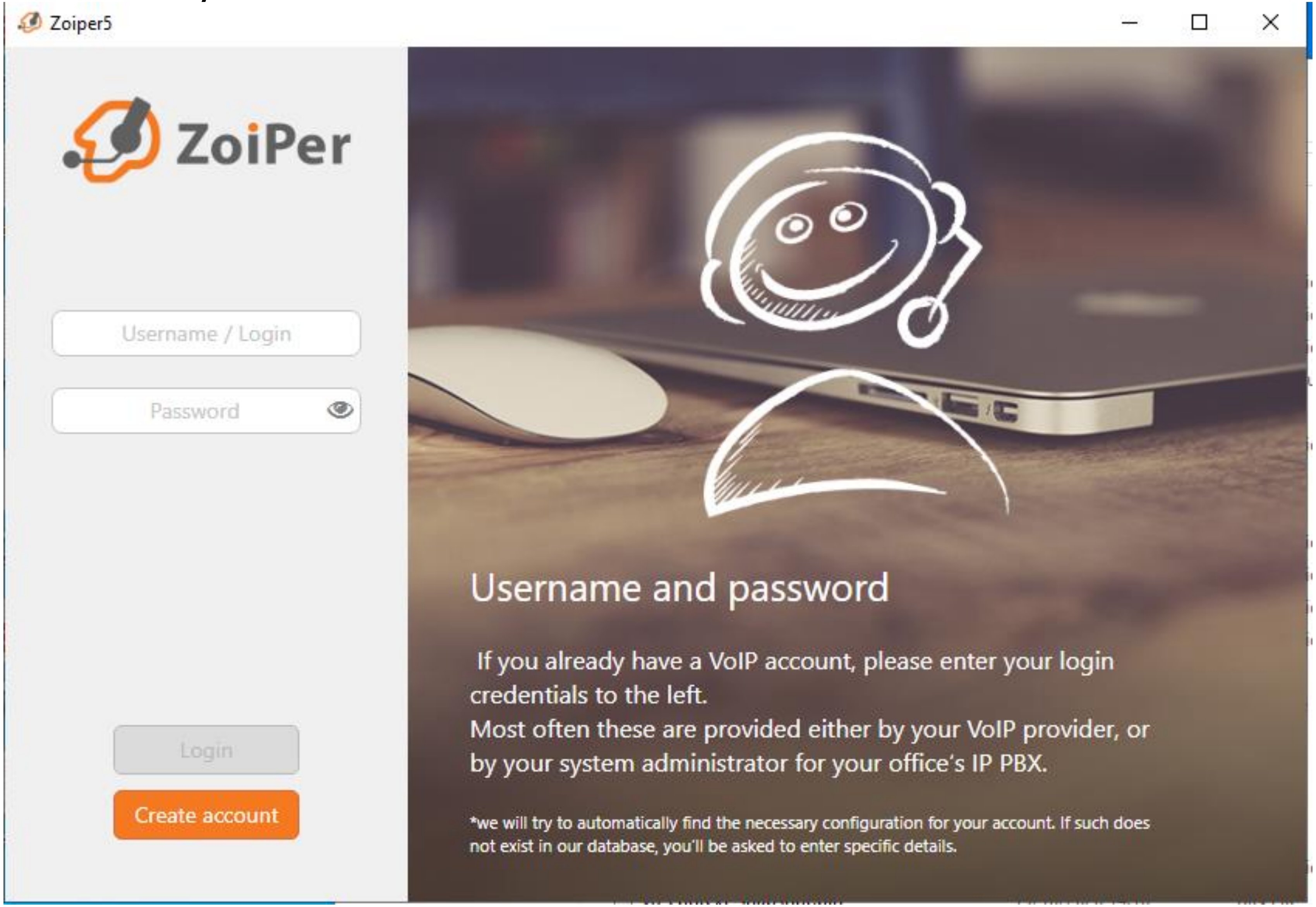
Source Name	S	C	O	E-Mail From	Subject	Date Received	Message ID	Path
nathanspireMS@gmail.com.ost	▽			bossoftheoperation@gmail.com	Mario Music	2020-11-02 15:57:56 GMT	2097252	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			sara.hoyle.personal@gmail.com	Payment	2020-11-02 16:00:36 GMT	2097284	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			bossoftheoperation@gmail.com	RE: Process Docs	2020-11-02 16:10:26 GMT	2097316	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			bossoftheoperation@gmail.com	Holiday Picture - India Gate	2020-11-02 16:15:57 GMT	2097348	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			bossoftheoperation@gmail.com	RE: Monthly revenue	2020-11-02 16:17:54 GMT	2097380	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			bossoftheoperation@gmail.com	Mario Music	2020-11-02 15:57:56 GMT	2097476	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			sara.hoyle.personal@gmail.com	Payment	2020-11-02 16:00:36 GMT	2097508	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			bossoftheoperation@gmail.com	RE: Process Docs	2020-11-02 16:10:26 GMT	2097540	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			bossoftheoperation@gmail.com	Holiday Picture - India Gate	2020-11-02 16:15:57 GMT	2097572	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			bossoftheoperation@gmail.com	RE: Monthly revenue	2020-11-02 16:17:54 GMT	2097604	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			nathanspirems@gmail.com	Holiday Picture	2020-11-02 16:07:09 GMT	2097668	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			nathanspirems@gmail.com	Process Docs	2020-11-02 16:10:03 GMT	2097700	\\Root - Mai
nathanspireMS@gmail.com.ost	▽			nathanspirems@gmail.com	Monthly revenue	2020-11-02 16:17:13 GMT	2097732	\\Root - Mai

Figure 9: Emails



Source Name	S	C	O	Account Type	ID	Data Source
nathanspireMS@gmail.com.ost			1	EMAIL	bossoftheoperation@gmail.com	Stockholm Case Image.E01
nathanspireMS@gmail.com.ost			0	EMAIL	sara.hoyle.personal@gmail.com	Stockholm Case Image.E01
nathanspireMS@gmail.com.ost			0	EMAIL	nathanspirems@gmail.com	Stockholm Case Image.E01

Figure 10: Emails Listed

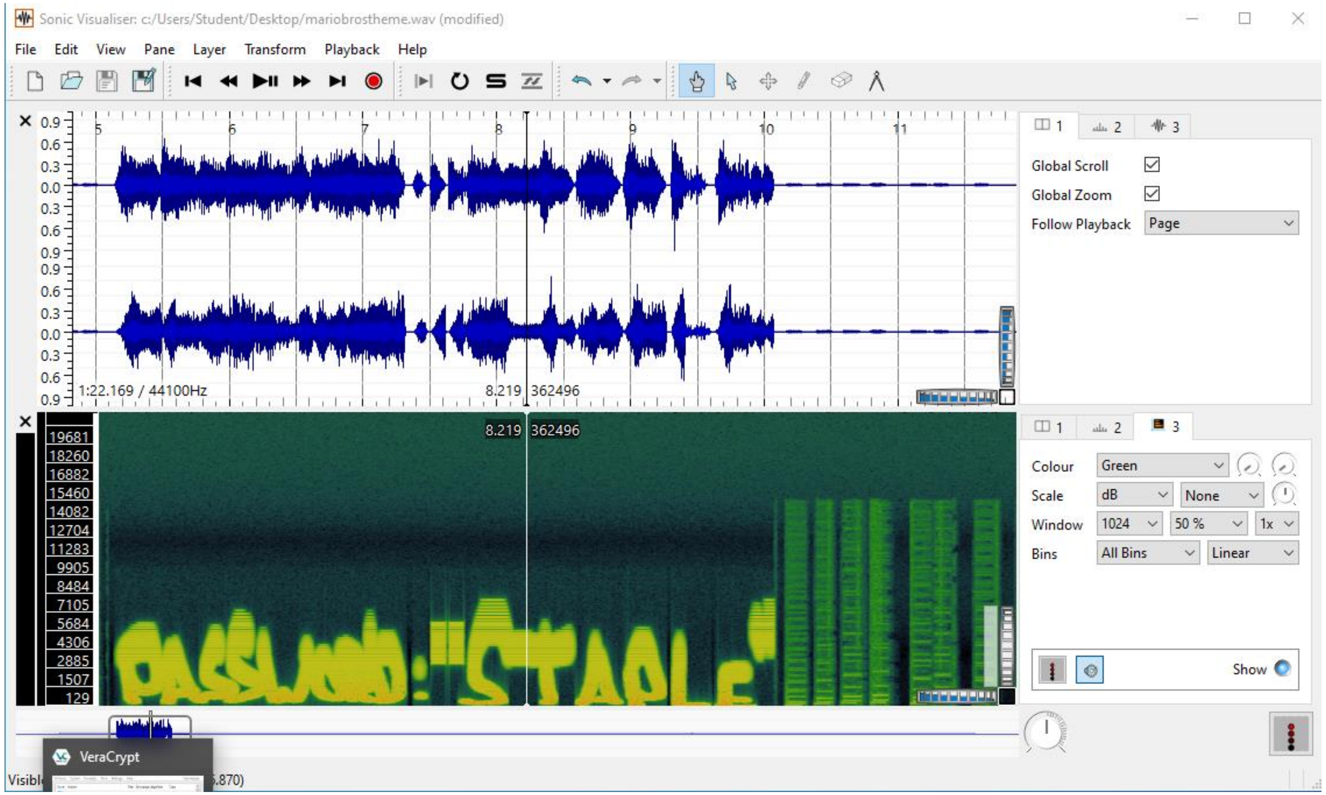


Username and password

If you already have a VoIP account, please enter your login credentials to the left.
Most often these are provided either by your VoIP provider, or by your system administrator for your office's IP PBX.

*we will try to automatically find the necessary configuration for your account. If such does not exist in our database, you'll be asked to enter specific details.

Figure 11: .exe Application Used



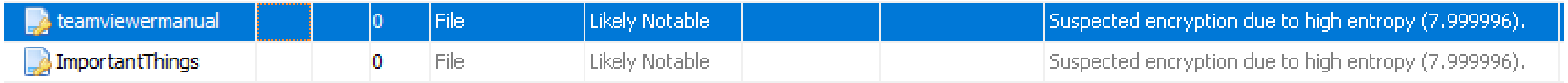
Sonic Visualiser: c:/Users/Student/Desktop/mariobrostheme.wav (modified)

Global Scroll ☑
Global Zoom ☑
Follow Playback: Page

Colour: Green
Scale: dB, None
Window: 1024, 50 %, 1x
Bins: All Bins, Linear

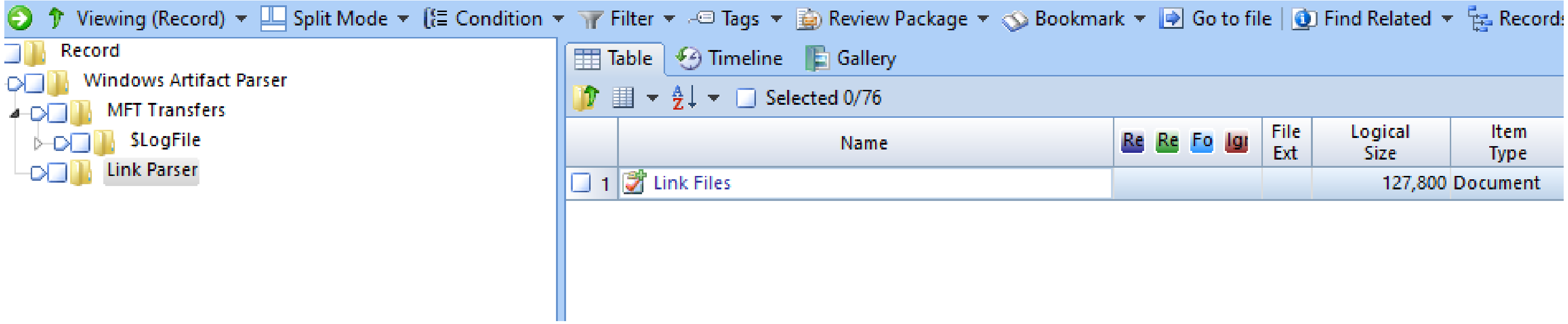
Figure 12: Hidden Message in audio file

Figure 13: Stegged Image



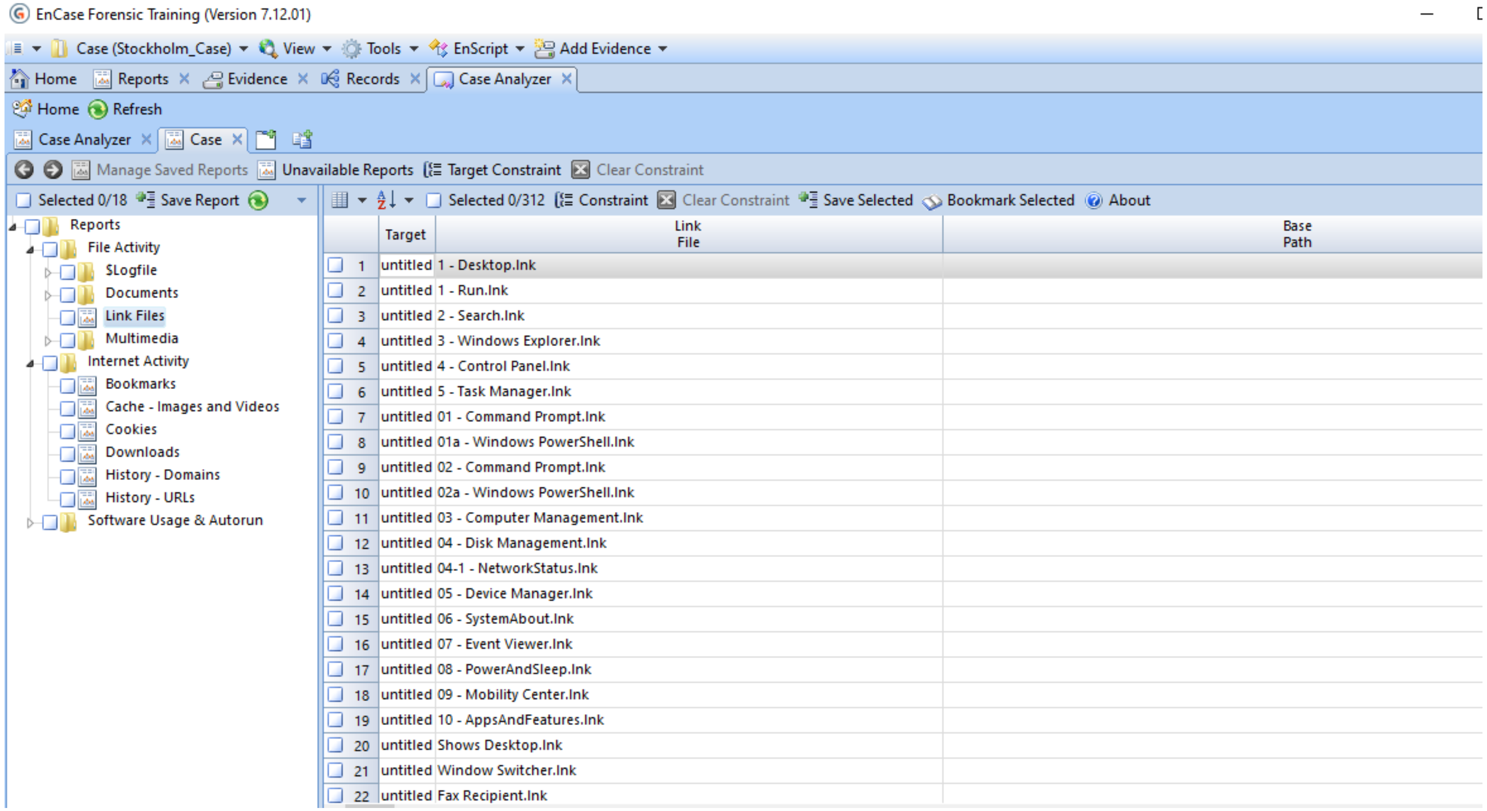
teamviewermanual		0	File	Likely Notable			Suspected encryption due to high entropy (7.999996).
ImportantThings		0	File	Likely Notable			Suspected encryption due to high entropy (7.999996).

Figure 14: Encrypted Files



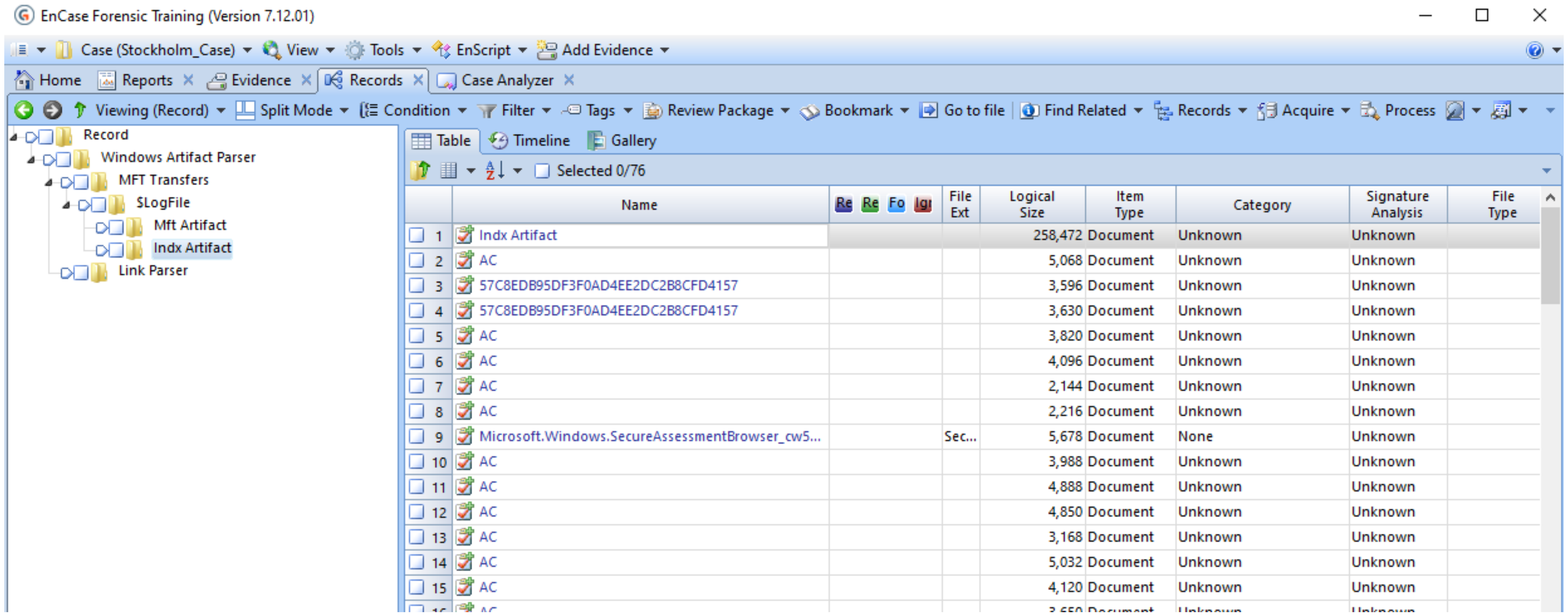
	Name	Re	Re	Fo	Igi	File Ext	Logical Size	Item Type
□ 1	Link Files						127,800	Document

Figure 15: Link Files


EnCase Forensic Training (Version 7.12.01)
Case (Stockholm_Case) View Tools EnScript Add Evidence
Home Reports Evidence Records Case Analyzer
Home Refresh
Case Analyzer Case
Manage Saved Reports Unavailable Reports Target Constraint Clear Constraint
Selected 0/18 Save Report
Selected 0/312 Constraint Clear Constraint Save Selected Bookmark Selected About
Reports
File Activity
$Logfile
Documents
Link Files
Multimedia
Internet Activity
Bookmarks
Cache - Images and Videos
Cookies
Downloads
History - Domains
History - URLs
Software Usage & Autorun

	Target	Link File	Base Path
1	untitled	1 - Desktop.lnk	
2	untitled	1 - Run.lnk	
3	untitled	2 - Search.lnk	
4	untitled	3 - Windows Explorer.lnk	
5	untitled	4 - Control Panel.lnk	
6	untitled	5 - Task Manager.lnk	
7	untitled	01 - Command Prompt.lnk	
8	untitled	01a - Windows PowerShell.lnk	
9	untitled	02 - Command Prompt.lnk	
10	untitled	02a - Windows PowerShell.lnk	
11	untitled	03 - Computer Management.lnk	
12	untitled	04 - Disk Management.lnk	
13	untitled	04-1 - NetworkStatus.lnk	
14	untitled	05 - Device Manager.lnk	
15	untitled	06 - SystemAbout.lnk	
16	untitled	07 - Event Viewer.lnk	
17	untitled	08 - PowerAndSleep.lnk	
18	untitled	09 - Mobility Center.lnk	
19	untitled	10 - AppsAndFeatures.lnk	
20	untitled	Shows Desktop.lnk	
21	untitled	Window Switcher.lnk	
22	untitled	Fax Recipient.lnk	

Figure 16: Link Files


EnCase Forensic Training (Version 7.12.01)
Case (Stockholm_Case) View Tools EnScript Add Evidence
Home Reports Evidence Records Case Analyzer
Viewing (Record) Split Mode Condition Filter Tags Review Package Bookmark Go to file Find Related Records Acquire Process
Record
Windows Artifact Parser
MFT Transfers
$LogFile
Mft Artifact
Indx Artifact
Link Parser
Table Timeline Gallery
Selected 0/76

		Name	Re	Re	Fo	Igi	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type
☐	1	Indx Artifact						258,472	Document	Unknown	Unknown	
☐	2	AC						5,068	Document	Unknown	Unknown	
☐	3	57C8EDB95DF3F0AD4EE2DC2B8CFD4157						3,596	Document	Unknown	Unknown	
☐	4	57C8EDB95DF3F0AD4EE2DC2B8CFD4157						3,630	Document	Unknown	Unknown	
☐	5	AC						3,820	Document	Unknown	Unknown	
☐	6	AC						4,096	Document	Unknown	Unknown	
☐	7	AC						2,144	Document	Unknown	Unknown	
☐	8	AC						2,216	Document	Unknown	Unknown	
☐	9	Microsoft.Windows.SecureAssessmentBrowser_cw5...					Sec...	5,678	Document	None	Unknown	
☐	10	AC						3,988	Document	Unknown	Unknown	
☐	11	AC						4,888	Document	Unknown	Unknown	
☐	12	AC						4,850	Document	Unknown	Unknown	
☐	13	AC						3,168	Document	Unknown	Unknown	
☐	14	AC						5,032	Document	Unknown	Unknown	
☐	15	AC						4,120	Document	Unknown	Unknown	
☐	16	AC						3,650	Document	Unknown	Unknown	

Figure 17: Artifacts Found

EXPORT:

Autopsy Generated Excel Report: https://uweacuk-my.sharepoint.com/:x:/g/personal/hamza2_wakili_live_uwe_ac_uk/Ec1Pii6UbjBNk3hO-2QV16cBZdOE2bVkNjewzHmZTRi71g?e=4eZgZp

Encase Report: Stockholm_Case.pdf